Anno 2 – N. 28
19 Giugno - 3 Luglio 2003

Boss: theguilty@hackerjournal.it

Editor: grand@hackerjournal.it,

Contributors: Bismark.it, DaMe`, Roberto 'dec0der' Enea, G14N, Il Coccia, Lidia, M4TT, nortoz, Robin, 3d0, Marco Triverio, S.D.S. KoRn.

DTP: Cesare Salgaro

Graphic designer: Dopla Graphic S.r.l. info@dopla.com

Copertina: Zocdesign.com

Publishing company
4ever S.r.l.
Via Torino, 51
20063 Cernusco S/N (MI)
Fax +39/02.92.43.22.35

Printing
Stige (Torino)

Distributore
Parrini & C. S.PA.
00189 Roma - Via Vitorchiano, 81-
Tel. 06.33455.1 r.a.
20134 Milano, viale Forlanini, 23
Tel. 02.75417.1 r.a.
Pubblicazione quattordicinale registrata al Tribunale di Milano il 25/03/02 con il numero 190.
Direttore responsabile Luca Sprea

Gli articoli contenuti in Hacker Journal hanno uno scopo prettamente didattico e divulgativo. L'editore declina ogni responsabilita' circa l'uso improprio delle tecniche che vengono descritte al suo interno. L'invio di immagini ne autorizza implicitamente la pubblicazione gratuita su qualsiasi pubblicazione anche non della 4ever S.r.l.

Copyright 4ever S.r.l.
Testi, fotografie e disegni, pubblicazione anche parziale vietata.

HJ: INTASATE LE NOSTRE CASELLE

Ormai sapete dove e come trovarci, appena possiamo rispondiamo a tutti, anche a quelli incazzati.

redazione@hackerjournal.it

hack'er (hãk'∂r)

"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."

IL COSTO DELLA MUSICA

Recentemente, anche per rispondere a qualche lettera, come quelle che trovate nelle prossime pagine, ho visitato nuovamente il sito della Federazione Industria Musicale Italiana. Lì, precisamente all'indirizzo www.fimi.it/dettaglio_documento.asp?id=319&idtipo_documento=4 c'è un comunicato che illustra una ricerca di PriceWaterhouse Cooper sul mercato discografico in Italia nel 2002. Riporta dati interessanti, che vorrei provare a interpretare anche se non sono un analista economico di quel particolare settore.

Sostanzialmente, l'analisi rivela che nel 2002, è cresciuto il numero dei dischi venduti, anche se il fatturato è rimasto inalterato. Secondo la Fimi, questo è dovuto al fatto che –per fronteggiare la crisi– le aziende hanno dovuto abbassare il prezzo dei dischi. Quindi si vende di più, ma si guadagna uguale. Tutto ciò è senza dubbio vero nell'insieme dei dati: "complessivamente il mercato cresce del 7,34% a unità vendute e dello 0,52% a valore", dice il rapporto, che afferma anche che "Le unità vendute nell'anno appena trascorso sono state in totale 47 milioni circa rispetto ai 43 milioni del 2001".

Analizzando più in dettaglio, però si scopre che gli album su CD, la fetta più importante del mercato, crescono del 17,58% a unità (numero di CD venduti) e del 6,52% come valore (euro incassati).
Quasi raddoppia il settore dei video musicali (grazie ai DVD, +93% a unità, +47% come valore), e persino il settore della musica classica (+76% di CD venduti, e +14% di fatturato), anche se ciò avviene dopo quattro anni di calo costante. E crescono anche i CD di repertorio a prezzo medio, cioè gli album vecchi venduti a prezzo ribassato.

In tutti i segmenti che abbiamo visto, sono cresciuti sia il numero dei dischi venduti, sia gli incassi per i produttori. Dove sta allora la grande crisi dovuta alla pirateria, di cui tanto si parla? Sostanzialmente, dai dati forniti, le perdite si concentrano in due punti: i singoli, che calano del 17,75% a unità e del 15,99% a valore, e le novità, che diminuiscono del 9% a valore e del 5,62% come unità vendute.

Guarda caso, questi due segmenti sono i più direttamente influenzati dalla pubblicità e dalla tradizionale promozione (passaggi radio, comparse in TV, partecipazione a festival canori…). Sono i settori in cui di solito dominano i successi di una stagione, i tormentoni dell'estate, spesso dal dubbio contenuto artistico.

A mio avviso, i sistemi di scambio di file hanno permesso a molte persone di conoscere artisti che non passano per radio, non conquistano la copertina di TV Sorrisi e Canzoni, non vanno al Festivalbar. E queste persone stanno comprando i loro dischi, come è giusto che sia, anche se sono vecchi (facendo crescere il settore del "repertorio").

E queste stesse persone stanno in parte snobbando le novità (perché hanno trovato di meglio), o forse semplicemente, le novità le scaricano da Internet perché ritengono che questi dischi "non vale la pena di comprarli". Tanto devono durare solo lo spazio di un'estate. Diverso è per il CD dell'artista preferito, che è bello possedere e collezionare, anche se la prima pubblicazione risale a tre, tredici o trenta anni fa.

Credo che da questo quadro, i discografici debbano imparare qualcosa: il pubblico è meno disposto di un tempo ad acquistare quelli che una volta erano "i singoli di successo", spesso costruiti in laboratorio. I gusti si stanno diversificando, e se si offre possibilità di scoprire artisti meno celebri, o di conoscere qualche grande del passato, i consumatori sono ben lieti di acquistarne i dischi (sempre che il prezzo non sia eccessivo).

Sull'ultimo punto del costo dei dischi spezzo una lancia a favore dei discografici, che da anni chiedono che venga annullata quella che è una grande ingiustizia legislativa: a differenza dei libri, e altri prodotti culturali, per i quali si applica l'Iva al 4%, i dischi hanno invece un aggravio del 20%, come qualsiasi altro prodotto. Se finalmente si decidesse a considerare i CD alla stregua di qualsiasi altro prodotto culturale, invece che un bene voluttuario, il costo di un CD da 20 euro si ridurrebbe all'istante a 16,60 euro, dando una ulteriore spinta a questo settore.

Ora, visto che ultimamente vengo spesso equivocato, faccio una precisazione: non sto giustificando la pirateria (a scopo di lucro o gratuita), né tanto meno istigando nessuno a copiare illegalmente la musica. Mi limito a osservare un fenomeno.

grand@hackerjournal.it

03_05_hj28_posta 11-06-2003 10:08 Pagina 3

Saremo di nuovo in edicola Giovedì 3 luglio !

IL CORAGGIO DI OSARE: INDIPENDENTI DA TUTTI

Hackerjournal.it, il muro per i tuoi graffiti digitali

w w w . h a c k e r j o u r n a l . i t

TRY2HACK RELOADED: METTITI ALLA PROVA!

TRY2HACK RELOADED

VUOI SAPERE E FAR SAPERE QUANTO SEI BRAVO? METTITI ALLA PROVA CON L'HACKGAME CHE VI PROPONIAMO IN COLLABORAZIONE CON GLESIUS

- DIECI LIVELLI UNO PIÙ TOSTO DELL'ALTRO
- UTILIZZO DI DIFFERENTI TECNICHE
- CLASSIFICHE DEI PUNTEGGI AGGIORNATE IN TEMPO REALE

Sulle riviste "normali", l'estate è il tempo di quiz e giochi. Noi non siamo da meno, ma se permettete, lo facciamo alla nostra maniera. Dal nostro sito potete raggiungere l'Hack Game di Glesius: per superare i vari livelli del gioco dovrete scavalcare i vari sistemi di protezione, individuando la password o sfruttando qualche bug per aggirare l'ostacolo.

Cosa si vince? Per ora, fama e gloria imperitura, oltre al gusto di aver misurato la propria abilità, ma stiamo studiando la possibilità di offrire ai più bravi qualche premio più sostanzioso.

Nuova password!

Ecco i codici per accedere alla Secret Zone del nostro sito, dove troverete informazioni e strumenti interessanti. Con alcuni browser, potrebbe capitare di dover inserire due volte gli stessi codici. Non fermatevi al primo tentativo.

user: ca6ficio
pass: bass8

FORUM: TUTTE LE AREE TEMATICHE

Forum

Generale

Annunci
Annunci dallo Staff.
Moderatore Carmageddon

Forum Generale
Di la tua sulla rivista... commenti,critiche per migliorare hj
Moderatori Carmageddon, Sismico

Try2hack
Consigli e tanto altro per risolvere il gioco!
Moderatori Carmageddon, Sismico

Uplink
Il forum sul gioco... consigli e tanto altro
Moderatori Carmageddon, Sismico

Filosofia Hacker
Il significato di "hacker",commenti,pensieri...
Moderatore Lord_Dex

In Edicola
Tutti i numeri commentati da voi...

Try2hack-Reloaded
Nuovo gioco di hj.it e glesius.it...

03_05_hj28_posta 11-06-2003 10:08 Pagina 4

mailto:
redazione@hackerjournal.it

ISTIGAZIONE 1

È la prima volta che do' una occhiata al vostro giornale, parlo proprio dell'ultimo numero, e devo mostrarmi inorridita al titolo in primo piano "Copia i CD Protetti - è un nostro diritto". Ho letto anche di sfuggita l'articolo, ma ho subito voluto scrivervi per porvi delle critiche.
E' ovvio che c'è libertà di parola e di opinione, ma francamente dubito che ci sia "libertà di istigazione alla pirateria". Dubito che la copia di un CD sia realmente "un nostro diritto". È ovvio che voi, sotto sotto, possiate giustificarvi parlando di diritto di preservare un proprio acquisto; se si rovina un CD è difficile poterlo riaverlo senza ricomprarlo, e su questo non ci piove. Ma dubito che sproteggere un CD protetto non è l'unico modo per preservare il contenuto. Esistono i tape deck collegabili alla sorgente audio di un lettore CD, esistono i minidisc, esiste l'acquisizione dati tramite scheda audio del PC, tutti strumenti con i quali si possono ottenere risultati soddisfacentissimi.
Ecco perché si poteva evitare a mio parere un titolo in copertina così esplicitamente aggressivo: c'è il diritto di preservare il proprio acquisto con i metodi che sopra ho descritto, c'è il rischio che la pirateria selvaggia rischierebbe il tracollo del sistema, la chiusura dei negozi del settore, la perdita in termini economici e di risorse di lavoro e soprattutto favorisce la diffusione di una mentalità che NON deve diventare diffusa, cioè che se un qualcosa si può copiare è meglio averla copiata che comprarla. La vostra rivista non può dimenticare di ricordare tutto questo.

Annarella C. (Anny)

ISTIGAZIONE 2

Informaticamente parlando sarete forse preparati ma dal punto di vista giuridico credo che abbiate parecchie lacune e infatti in merito al punto dove dichiarate (HJ 27, pag.2): "La sensazione generalizzata (ma di chi?) infatti è che le forze dell'ordine invece di garantire il monitoraggio costante delle attività legali, punendo sistematicamente...". Ma vi dice qualcosa l'omissione di atti d'ufficio che è un reato gravissimo per un pubblico ufficiale? E che obbligato in virtù di una denuncia a svolgere le indagini? Questo forse, spremendo un attimino le meningi non vi fa pensare che la MD4 abbia denunciato tale fatto alle autorità e che quest'ultime non abbiano potuto fare a meno di intervenire per non incorrere alle omissioni poc'anzi descritte? Ma vi rendente conto prima di premere un bottone sulla tastiera quali assurdità dichiarate alla povera gente credulona quando poi voi istigate con titoli illusori a diventare hacker in dieci mosse (è un reato anche l'istigazione a commettere dei delitti se questo non lo sapete, quindi la polizia dovrebbe indagare prima voi). Comunque se aspettavate quest'evento per denigrare le forze dell'ordine avete veramente poco gusto e soprattutto poca intelligenza con questo concludo dicendovi che non sprecherò mai più un centesimo di euro per leggere le vostre C......!!!!

Enzo

Visto l'argomento simile, diamo una sola risposta a due diverse lettere. La nostra posizione è sempre stata molto chiara: le leggi si possono criticare (e infatti lo facciamo), ma vanno rispettate. Sfido chiunque a trovare nelle 896 pagine di Hacker Journal pubblicate finora, una sola riga in cui istighiamo i lettori a compiere un crimine. Non lo abbiamo mai fatto, né mai lo faremo, quindi restituisco al mittente l'invito a pensare a fondo prima di scrivere parole pesanti.
Riguardo alla copia di CD audio, la legge è inequivocabile:
"Decreto legislativo 09.04.2003 n° 68, Art. 71-sexies - 1. E' consentita la riproduzione privata di fonogrammi e videogrammi su qualsiasi supporto, effettuata da una persona fisica per uso esclusivamente personale, purché senza scopo di lucro e senza fini direttamente o indirettamente commerciali, nel rispetto delle misure tecnologiche di cui all'articolo 102-quater".
E altrettanto chiari siamo stati quando abbiamo detto che, invece, la rimozione delle tecnologie per il DRM da contenuti concessi con licenze particolari, per esempio "a tempo" (file Wma, eBook eccetera) è sempre un reato, e quindi non va fatto.
Riguardo al presunto collasso dell'industria musicale, rimando all'editoriale di questo numero, a pagina 2.
Passando poi all'editoriale del numero scorso, nessuno ha criticato le Forze dell'Ordine per il fatto di aver indagato e catturato i due ragazzi, e anzi nell'articolo dico testualmente "Quest'ultima parte non vuole assolutamente essere una giustificazione all'operato dei due lamerozzi. Han fatto una cazzata, ed è giusto che ne paghino le conseguenze."
Il punto è che queste cose non finiscono sui quotidiani e sui TG nazionali se non vengono adeguatamente spinte e sponsorizzate: comunicati, conferenze stampa, dichiarazioni, interviste... E di questo ritengo responsabili non gli ufficiali che hanno condotto le indagini, che hanno fatto solo il loro dovere, ma chi si occupa della relazioni con la stampa.
È giusto dipingere due minorenni come pericolosissimi criminali informatici, facendo in modo che la notizia abbia così tanto risalto? Seguo questo argomento da anni, e ti assicuro

☺ Tech Humor ☺

Avreste investito in questa azienda? Si tratta dello staff di Microsoft, nel 1978. Bill Gates è il primo in basso da sinistra.

LA FAMIGLIA DI MAYALINUX

Cara redazione di HJ, complimenti per la rivista, vi seguiamo dal primo numero, siamo una famiglia "digitalizzata": io sono un reverse engineer (un ingegnere con la passione del contrario ;), mio fratello è un un OdontoHacker (un odontotecnico con la passione della vostra rivista), mia mamma ci chiama con un sistema radiocontrollato e il mio papà lo sentiamo via email visto che è emigrato, e, come ogni buona famiglia abbiamo il nostro bravo animaletto: è un incrocio fra un maiale ed un "pinguino", il suo nome è MAYALINUX...
E' un PC un po' datato(P 166MHz), prontamente overclockato ad 250 MHz con 96 MB di RAM arrangiata qua e là, un HD di 6 GB e quant'altro siamo riusciti a mettere insieme con l'aiuto di alcuni amici. L'OS è la versione Mandrake 8.1 di linux e in rete va una scheggia. L'esterno è stato curato interamente a mano da mio fratello con della resina per dentiere (infatti ha un sorriso smagliante) anche se ancora manca di qualche ritocchino qua e la....
Se proprio non volete pubblicarlo (cosa che provocherebbe il suicidio dell'odontohacker...) almeno fatevi due risate con il nostro animaletto da compagnia MAYALINUX.

Xastarot & OdontoHacker

che è una cosa che ho osservato spesso, in Italia come all'estero, nell'ambito del crimine informatico: titoli roboanti, accuse pesantissime, che spesso si sgonfiano in aula. O, peggio, si traducono in condanne sproporzionate rispetto ai crimini effettivamente commessi, proprio per via delle campagne di stampa. Tutto per la voglia di protagonismo di un procuratore, o di un corpo di polizia (leggiti le cronache dell'operazione Sundevil negli anni 90 in USA, e le altre storie raccontate su "Giro di vite contro gli Hacker", di Bruce Sterling).

IP, EMAIL E VENDETTA

Cara redazione,
qualcuno (così è scritto sulla descrizione dell'infiltrazione del mio firewall, ossia sygate) sta scannerizzando il tuo computer...
Il mio firewall è riuscito a localizzare il suo indirizzo IP, ebbene, la mia domanda è, con il suo IP, potrei fare qualcosa per vendicarmi, risalendo a questo tizio?
Da come ho sentito l'indirizzo IP è molto prezioso, quindi, potrei fare qualcosa per fargliela pagare per mezzo di questo indirizzo... magari spedendogli direttamente una e-mail, per mezzo del suo indirizzo IP...

Non puoi "contrattaccare" chi ti sta attaccando, perché compiresti un reato tu stesso. L'unica cosa che si può fare a seguito di un attacco, è prendere provvedimenti sul proprio computer per evitare che l'attacco continui, ed eventualmente rivolgersi alle forze dell'Ordine, sporgendo denuncia. In questo caso, però, il portscanning in sé non è un'attività ad alto rischio: è un po' come sporgere denuncia perché qualcuno ha chiamato il tuo telefono: può aver sbagliato numero, oppure essere semplicemente un burlone in vena di scherzi telefonici. Se le "telefonate" si fanno insistenti e fastidiose, allora è il caso di fare qualcosa.
Da un indirizzo IP non si può risalire all'indirizzo email di una persona, come chiedi tu, se non in casi rarissimi (nel caso in cui l'indirizzo IP corrisponda a un nome di dominio, registrato a nome della persona che stai cercando).

APACHE E PHPINFO

Cercando un testo musicale con Google, ho trovato una pagina chiamata Phpinfo e che riporta un sacco di informazioni sulla configurazione del server. Ma, teoricamente, questa pagina non dovrebbe essere inaccessibile agli utenti normali?

Metallized Blood

Dipende da come è configurato il server. Solitamente, phpinfo è una pagina che serve a fare una diagnostica del sito, analizzando tipo e versione dei vari pacchetti che servono al funzionamento di PHP.
Niente impedisce di rendere pubblici questi dati (non ci sono informazioni critiche per la sicurezza, come password o account utente), ma in effetti non è una buona idea, perché fornisce a eventuali cracker informazioni utili a preparare un attacco.
In linea generale, se si vuole mantenere la pagina sul sito, conviene nasconderla in una directory non facilmente raggiungibile. Sebbene la logica suggerirebbe di escludere questa directory dai motori di ricerca, inserendola nel file robots.txt, questa non è una buona idea: un attaccante potrebbe infatti leggere il contenuto del file robots.txt, e indovinare la posizione delle cartelle con contenuti accessibili ma che si vogliono mantenere riservati, vanificando le nostre intenzioni. La cosa giusta da fare, quindi, è semplicemente quella di evitare di linkare la pagina o la cartella ad altre pagine del sito, accessibili pubblicamente. Gli spider non riusciranno a trovarla.

☺ Tech Humor ☺

Attenzione: c'è in giro un nuovo virus che colpisce i mouse!

NEWS

NUMERI

DATI E STATISTICHE

30 sessioni
Numero medio di collegamenti Internet al mese negli USA.*

9723
Messaggi email arrivati alla redazione di Hacker Journal nell'ultimo anno.

25 ore, 13 minuti, 52 secondi
Tempo speso su Internet da casa, sempre negli USA.*

8 ore
Tempo medio in cui i redattori di HJ sono collegati a Internet quotidianamente, weekend compresi.

31 minuti e 48 secondi
Tempo medio di una sessione su Internet negli USA.*

55 secondi
Tempo medio di permanenza su una pagina Web.*

7 secondi
Intervallo di tempo tra il login di PasseraScopaiola sul canale #sbattipanza e la prima domanda "da dove dgt?"

121.934.611
Numero di apparecchi digitali collegati a Internet negli USA.*

13
Numero di finestre che bisogna chiudere dopo aver aperto la home page di sessogratis.it

1:25
Rapporto tra le righe di testo originali e quelle "quotate" nel messaggio di un troll.

2:1
Rapporto tra le righe di contenuto e quelle della signature in un messaggio di un narcisista.

*: fonte: Nielsen/NetRatings

RETATA SUL PEER2PEER. ANZI, NO.

Nelle scorse settimane, nella piccola ma ormai frequentata Rete italiana si è sparso il panico. Repubblica prima, e vari altri siti di informazione poi, hanno pubblicato il resoconto di un'operazione del Nucleo operativo provinciale di Milano della Guardia di Finanza, contro la pirateria software e musicale. Si parlava di 75 persone già denunciate per violazione di diritto d'autore e ricettazione, e circa 3000 che stavano per essere identificate e denunciate.
Per come veniva raccontata la vicenda, sembrava proprio che gli inquirenti stessero setacciando le reti Peer 2 Peer, e in effetti l'articolo parlava di gente comune finita tra gli indagati: professionisti, studenti, impiegati, e persino due marescialli dei Carabinieri. Migliaia di persone hanno temuto di finire in galera solo per aver usato qualche programma di scambio file come WinMX, Kazaa o uno dei vari client Open Nap.
A leggere bene l'articolo di Repubblica, però, c'era qualcosa di strano: imprecisioni tecniche, dettagli apparentemente inspiegabili in quel contesto, come l'uso di email cifrate tra "fornitori e clienti" (sic).
Beh, è bastato attendere il comunicato stampa ufficiale della Guardia di Finanza per vedere sgonfiare, come spesso accade, una notizia gonfiata all'inverosimile. L'operazione della GdF, infatti, era mirata a dei veri e proprio pirati, che masterizzavano e vendevano software illegale in grande quantità. Il P2P c'entra solo perché era il principale canale di approvvigionamento dei software, della musica e dei film che poi venivano masterizzati e venduti a caro prezzo. Per alcuni dei pirati, gli introiti arrivavano a 25.000 euro al mese, e la GdF stima un giro di affari annuo complessivo del gruppo di 100 milioni di euro.
Un consiglio a Repubblica e agli altri siti e giornali che si sono limitati a copiare da loro: in giro ci sono bravi giornalisti che l'informatica e Internet li conoscono bene. Perché non lasciarle scrivere a loro certe cose?

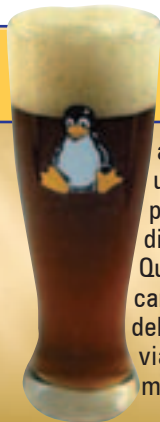
HACKMEETING 2003

È stato definito solo all'ultimo momento il luogo in cui si terrà l'hackmeeting 2003, tradizionale incontro delle comunità e delle controculture digitali italiane. L'appuntamento è al centro giovanile Barrio, nell'ex scuola elementare di Strada Cuorgnè 81, a nord di Torino.
Gli organizzatori promettono tre giorni di seminari, giochi, feste, dibattiti, scambi di idee e apprendimento collettivo, e come al solito il cuore del meeting sarà il "lan space", spazio dove ognuno può portare il proprio computer e collegarsi in rete con gli altri, sperimentando, giocando e condividendo gratuitamente i propri materiali. Tutte le informazioni su www.hackmeeting.org

BUGBEAR TORNA A FAR DANNI

Tra I worm che hanno contagiato milioni di utenti via posta elettronica negli ultimi anni, Bugbear è stato sicuramente uno dei più fastidiosi, e potenzialmente pericolosi. Ultimamente il bastardo è tornato alla grande a infestare reti e computer, con la sua variante Bugbear.b. La pericolosità del virus è dovuta a vari fattori. Innanzi tutto, installa nel computer una backdoor che permette a un cracker di collegarsi al computer colpito e prelevare informazioni riservate, password cifrate comprese, grazie anche alla sua funzionalità di keylogger (registrazione dei tasti premuti dall'utente). Se questo non bastasse, la riservatezza dei dati personali è messa a rischio anche da un altra "funzionalità": per risultare più credibile durante il contagio a nuovi destinatari, il virus preleva porzioni di messaggi dall'archivio email della vittima, crea un nuovo messaggio con indirizzo casuale, e vi allega un file preso anch'esso a caso (file che ovviamente ha provveduto a "patchare" con il codice virale). È ovvio che questi messaggi e questi file potrebbero arrivare a persone, conoscenti della prima vittima, alle quali non erano minimamente destinati: coniugi infedeli, attenti!

LINUX ÜBER ALLES

Il comune di Monaco di Baviera ha deciso di far migrare i 14.000 computer dei suoi uffici su Linux e software libero, abbandonando la piattaforma Microsoft. Un gruppo di analisi ha fatto uno studio che ha assegnato 6.218 punti su 10.000 a Linux, e 5293 a Microsoft. Pare che lo stesso Steve Ballmer, CEO di Microsoft in quei giorni in vacanza in Europa, abbia interrotto le sue ferie per andare a fare al Consiglio Comunale un'offerta di quelle "che non si possono rifiutare", proponendo di fornire il software sotto costo. Questo però non è servito a far cambiare idea agli amministratori della città, che presto daranno il via alla lunga procedura di migrazione.

APPLE SI COMPRA NAPSTER?

Il punto di domanda è d'obbligo, perché la maggior parte delle indiscrezioni relative ad Apple spesso si rivela infondata, ma questa è la notizia che sta rimbalzando sui siti di "rumors". Apple starebbe infatti per acquisire Roxio, ex divisione di Adaptec, e produttrice di software per masterizzazione PC e Macintosh. Lo scorso anno, Roxio aveva acquistato Napster, e quindi Apple si porterebbe a casa anche il primo sistema di file sharing della storia, anche se ormai è un guscio vuoto il cui valore massimo è probabilmente il logo, oltre ovviamente ai dati statistici sull'uso del sistema. Il tutto potrebbe essere molto utile al nuovo servizio di vendita di brani musicali su Internet, incluso nella nuova versione di iTunes, il lettore Mp3 di Apple.

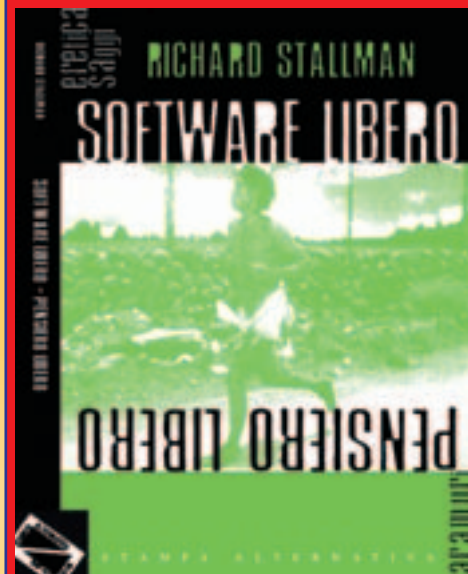
TCP METTE IL TURBO

La rivista New Scientist ha pubblicato un interessante articolo su una evoluzione del protocollo TCP, chiamata FastTCP, attualmente in fase sperimentale. Normalmente, in una connessione TCP, dopo che viene inviato un pacchetto di dati, il successivo pacchetto viene spedito solo dopo una conferma dell'avvenuta ricezione del primo. Se la "conferma" non arriva, il server dimezza la velocità e riprova a spedire il pacchetto. FastTCP invece cerca di stabilire a priori qual è la massima velocità che quella connessione può sostenere senza perdere dati, e invia i pacchetti a questo ritmo, decisamente più elevato. Il bello è che questo sistema può essere impiegato sui network e sulle infrastrutture attualmente in uso, senza bisogno di aggiornamenti.

Lo schema di funzionamento del protocllo FastTCP, attualmente in fase di sperimentazione, così come lo si può vedere all'indirizzo: www.newscientist.com/news/news.jsp?id=ns99993799

HOT!

STALLMAN IN ITALIANO

Stampa Alternativa ha pubblicato "Software Libero Pensiero Libero", a cura di Bernardo Parrella e dell'Associazione Software Libero, traduzione italiana di parte della raccolta di discorsi e saggi di Richard Stallman, "Free Software, Free Society: Selected Essays of Richard M. Stallman".

Nella versione italiana, il libro è stato infatti spezzato in due volumi. Il primo dei due, recentemente presentato, è in vendita al costo di 9 euro

IL P2P SI SUCCHIA TUTTA LA BANDA

Negli USA il traffico generato dallo scambio di file tra privati ha superato il 50% della banda attualmente disponibile. Secondo alcuni amministratori intervenuti in un dibattito su Slashdot.org, la situazione è ancora peggiore nelle università, dove la disponibilità di computer sempre accesi, e banda a volontà, attira molti utenti del Peer 2 Peer. C'è chi dice che bisogna mettere un freno al fenomeno, e chi invece pensa che sia ora di accendere qualche chilometro di fibra ottica in più, per aumentare la banda disponibile.

NEWS

HOT!

NON TUTTI GLI AGGIORNAMENTI VENGONO COL BUCO

Per fortuna non succede troppo spesso, ma gli aggiornamenti di Microsoft, a volte, riescono a creare problemi più gravi di quelli che dovrebbero risolvere. Una volta installata, una recente patch rilasciata per Windows XP causava la disconnessione immediata da Internet. In attesa dell'aggiornamento funzionante, l'unica cosa da fare è disinstallare quello venuto male.

LA GUERRA DEI PREZZI

È iniziata la corsa al ribasso delle tariffe per la musica scaricata a pagamento da Internet. Listen.com annuncia la possibilità di masterizzare un brano a 79 centesimi, venti in meno di quanti non ne chieda Apple col servizio iTunes. Attenzione però: mentre Apple fa pagare solo i singoli download, Listen.com impone un abbonamento al servizio che costa 9,95 dollari al mese.

CONNESSI DAPPERTUTTO

È stato finalmente firmato dal nostro ministro delle telecomunicazioni il decreto sulle Wireless Lan, che offre la possibilità ai gestori telefonici di fornire servizi a banda larga in modalità Wireless. Finisce dunque la fase di sperimentazione e si comincia a fare sul serio: l'era delle reti mobili basate su antenne è incominciata. In soldoni per noi cosa significa? Significa che potremo collegarci a Internet, scaricare email, giocare, lavorare in qualsiasi momento e ovunque ci troviamo: al bar, in aeroporto, allo stadio, purché il locale sia servito da un punto di accesso Wireless.

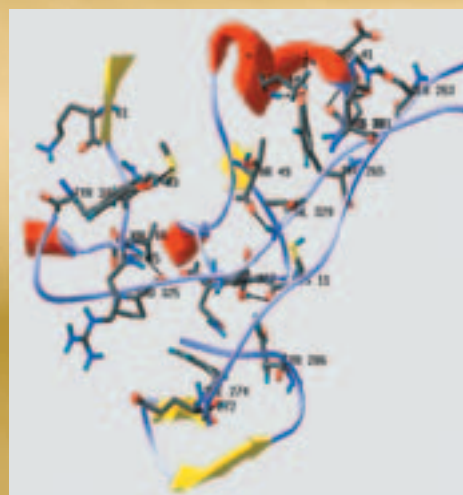
SVEGLIA O SEGRETARIA?...

Quante volte siamo arrivati al lavoro con ore di ritardo, giustificandoci con un candido: "C'era traffico"? Bene, prepariamoci a confezionare una nuova scusa, perché presto a questa non crederà più nessuno (se mai qualcuno ci ha creduto). Sta infatti per essere messa a punto dall'Università di Uxbridge una sveglia collegata a Internet che verifica le condizioni del traffico sulla strada da noi abitualmente percorsa. In caso di ingorgo, ci sveglierà in anticipo. Non solo: fornirà percorsi alternativi e potrà avvertire altre persone di nostri possibili ritardi. Meglio della più operativa delle segretarie, insomma. Se per disertare l'ufficio è una fregatura, l'aggeggio si rivelerà provvidenziale per tutti gli appuntamenti che non vogliamo perdere e, perché no, anche per le vacanze. Vi immaginate? Altro che partenze intelligenti: valige in macchina e poi tutti a letto. Quando è il momento buono per partire, ce lo dirà la sveglia. Se ci preparasse anche il caffè e poi chiudesse il gas, sarebbe davvero perfetta.

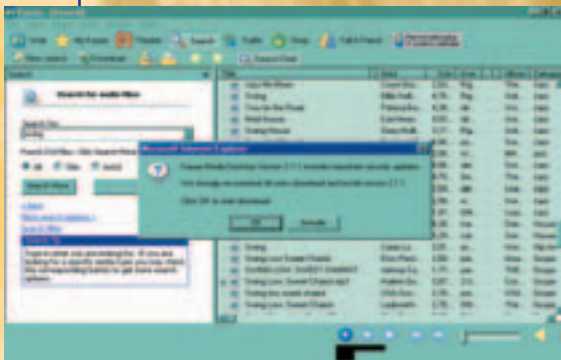
LAUREA IN VIRUS

Il vostro hobby è creare virus informatici ma siete a corto di idee? Non c'è problema: fate un giretto all'università di Calgary dove il prossimo autunno verranno istituiti corsi di "Computer Virus and Malware". Docenti preparatissimi insegneranno tutto quello che c'è da sapere sui virus: come si creano, quali tecnologie occorrono e via dicendo. Inutile dire che l'iniziativa è parsa bizzarra e ha suscitato polemiche a non finire nel mondo informatico. "Che bisogno c'è di diffondere informazioni su un problema già sufficientemente grave, come quello dei virus?", si è chiesto qualcuno. "Per creare cultura ed esperti nel settore", rispondono i promotori dell'iniziativa. Come dire: per difendere la nostra casa da possibili furti, bisogna sapere tutto su serrature e allarmi.

CYBER BATTERI

Le elezioni amministrative della settimana scorsa sono state le prime in cui è entrato in vigore un divieto piuttosto originale: quello di portare in cabina un cellulare con fotocamera. Il timore è che gli elettori possano documentare con una foto il momento del voto, permettendo così alla mafia che controlla i voti di verificare l'effettiva preferenza espressa. Ne hanno parlato un po' tutti, ma non è forse vero che la stessa cosa si può fare con una vecchia Polaroid, o con una qualsiasi macchina fotografica, digitale o no?

TORNA A CASA COMPUTER

Ti rubano il computer? Tranquillo: ci pensa TheftGuard a rintracciarlo e a farlo tornare a casa tua. Questa nuova diavoleria è un dispositivo di sicurezza messo a punto da Phoenix Technologies, noto produttore di BIOS, e Softex che invia il numero seriale del chip a un centro dati, ogni volta che il computer si collega a Internet. Se il numero corrisponde a quello di un PC rubato, scatta l'allarme e, tanto per cominciare, all'illegittimo utente viene bloccato completamente il sistema. Secondo, viene segnalato l'indirizzo IP da cui il ladro si è collegato, facilitando la polizia nell'opera di ritrovamento. Infine se il proprietario dovesse farne esplicita richiesta, in men che non si dica è possibile ordinare la cancellazione di tutti i dati contenuti sul PC trafugato. Come è ovvio, le perplessità e gli interrogativi sgorgano copiosi dalle nostre ben funzionanti testoline. Ci si chiede se tutto questo serva veramente o se non sia l'ennesima trovata dei Soliti Ignoti per controllare ogni nostro movimento elettronico.

SCAMBI CON FALLA

Teniamo d'occhio i messaggini inviatici da Kazaa e I-Mash, se usiamo uno di questi programmi per condividere file in Rete. È appena uscita una patch che risolve un problema di sicurezza evidenziato da un esperto di sicurezza, tale Random Nut.
La vulnerabilità, dice l'esperto in un messaggio postato sulla mailing list Full Disclosure, non è data da un bug dei programmi, bensì da una falla di Fast-Track, la tecnologia su cui poggiano molti dei software peer-to-peer. La falla potrebbe consentire a uno o più cracker di violare i computer degli utenti. I più a rischio sono i computer che nella rete Fast-Track hanno il ruolo di Super Node, funzione generalmente attivata sulle connessioni a banda larga . Anche se Fast-Track inizialmente ha cercato di minimizzare il problema, alla fine si è impegnata a risolvere l'inconveniente. Kazaa ha invece prontamente annunciato il rilascio di una patch nel giro di poche ore.

TICCHETTIO PERSONALIZZATO

Siamo abitudinari, noi appartenenti al genere umano. Tremendamente abitudinari. Tanto che se chiamati a premere una stessa sequenza di tasti su una tastiera, per esempio quelli che servono per digitare un codice, utilizziamo sempre il solito schema di digitopressione. Vale a dire che lo facciamo sempre allo stesso modo. Due scienziati hanno pensato di studiare il fenomeno e di utilizzarlo come sistema di riconoscimento. La durata della digitazione del codice e la pressione esercitata dalle dita sono state misurate e calcolate come facenti parte di un'onda. Ogni soggetto è dunque identificabile perché produce un'onda unica. Qualcosa di simile e per alcuni versi preoccupante fu annunciato nel 2000 da NetNanny, che provò a identificare un utente attraverso la tastiera, in modo da contrastare la pirateria informatica e musicale.

A ME GLI OCCHI

Per lasciarti entrare negli Stati Uniti gli americani l'han sempre fatta lunga. Prima dovevi dichiarare di non essere né nazista né comunista, poi controlli e domande a non finire. Adesso per ottenere un visto saremo obbligati a lasciare foto e impronte digitali. Non solo: a breve, è solo questione di perfezionamento delle tecnologie, si pensa alla possibilità di riconoscimento del volto e dell'iride e di richiesta informazioni dell'aspirante viaggiatore ai consolati americani nei paesi di origine del viaggiatore. Si salvi chi può.

EURO DELIRI

Prima o poi i microchip finiscono dappertutto. Questa volta è il turno delle banconote. A causa delle troppe falsificazioni, la Banca Centrale Europea sta giungendo a un accordo con Hitachi per inserire nelle banconote un microchip dello spessore di soli 0,4 millimetri. Naturalmente per verificare l'autenticità degli euro, occorrerà installare in banche, negozi e sportelli scanner in grado di rilevare il microchip. A qualcuno la faccenda puzza di mossa commerciale. Avete idea di che giro di soldi potrebbe esserci dietro l'acquisto (ovviamente a carico dei privati) di questi sistemi di rilevazione, nonché dietro la stampa di tante nuove banconote?

SUPER PIRATA IN MANETTE

Ha fatto danni per un miliardo di dollari ma finalmente è stato catturato. Si tratta di un pirata informatico ucraino di 25 anni che commerciava software illegale. Vysochansky, che si era guadagnato il posto nella lista dei dieci più ricercati dai servizi di sicurezza americani, è stato catturato a Bangkok. La lunga mano della giustizia americana arriva proprio ovunque…

10_11_hj28_eucd 11-06-2003 10:16 Pagina 10

EUCD: la fine della libertà

Le conseguenze della direttiva europea EUCD vanno ben più in là dell'aumento del costo dei supporti vergini.

Dallo scorso 29 aprile, i cd vergini costano di più, possederne uno pirata a casa o effettuare file sharing in rete è reato. Questi sono solo alcuni degli effetti della nuova normativa sul copyright, forse più nota a tutti come EUCD, ma di certo non i più gravi. Pochi sanno, infatti, che ad essere stati presi ingiustamente di mira **non sono solo le nostre tasche**: sono a rischio le nostre **libertà digitali**, il **futuro dello sviluppo** in campo informatico, **la libertà di ricerca ed espressione**.

>> Intimidazione e censura diventano legge

L'EUCD, **European Union Copyright Directive** (o direttiva 2001/29/CE del Parlamento Europeo e del Consiglio sull'"armonizzazione di taluni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione"), nasce con lo scopo di aggiornare ed uniformare le leggi europee sul diritto d'autore (europa.eu.int/information_society/ topics/multi/digital_rights/doc/directive_copyright_it.pdf), adeguandole ai trattati della World Intellectual Property Organization (www.wipo.org), nata nel 1996 per regolare i copyright nel mondo. Essa s'ispira ad un'altra legge in applicazione negli Stati Uniti, il DMCA, Digital Millennium Copyright Act, che è già stata utilizzata per l'intimidazione e persino l'arresto di ricercatori e sviluppatori (vedi il caso Sklyarov, www.freesklyarov.org), e per la censura di motori di ricerca, siti Internet, forum di discussione e programmi (www.anti-dmca.org). Se negli USA si ricordano soprattutto le battaglie di **Lawrence Lessig**, professore di diritto a Stanford (www.quintostato.it/archives/000157.html), in Italia non si può non citare l'**Associazione Software Libero** (www.softwarelibero.it/progetti/eucd) che ha promosso sin dall'inizio una campagna di sensibilizzazione sui pericoli dell'Eucd (Alceste Scalas www.softwarelibero.it/progettieucd/analisi.shtml). I pericoli dell'EUCD, secondo Alceste Scalas, sarebbero sostanzialmente tre. Se non vi si porrà rimedio, un giorno forse potrebbero tradursi in tre "divieti": **vietato conoscere, vietato esprimersi, vietato diffondere il "sapere"**.

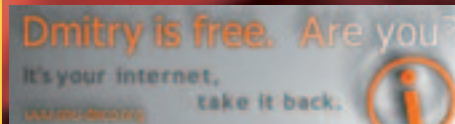
>> Vietato conoscere

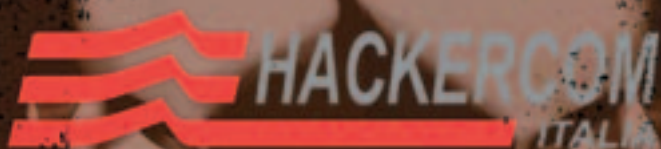
L'EUCD prevede delle sanzioni per chi aggira le "misure tecnologiche" (che altro non sono che semplici porzioni di programma) che servono a **regolare l'utilizzo e a impedire un uso non autorizzato del materiale** digitale coperto da diritti d'autore. Rende inoltre illegale **la creazione e la distribuzione** di qualunque strumento, sia hardware che software, in grado di agevolare l'operazione. Comprendere e studiare il funzionamento di un programma, analizzare il formato dei dati che esso trasmette e memorizza potrebbe dunque diventare un reato, benchè in un'altra direttiva, la 91/250/CEE, sia sancito come diritto.

10_11_hj28_eucd 11-06-2003 10:16 Pagina 11

A rischio vi sono **decompilazione e reverse-engineering**; quindi la creazione di software libero e, in particolare, lo sviluppo di programmi liberi interoperanti, che rischiano di non poter garantire, come finora è stato, una compatibilità con i formati ed i sistemi operativi proprietari più diffusi; le ricerche sulla **crittografia** e la **sicurezza informatica**, basate proprio sullo studio e sul superamento degli attuali sistemi di protezione. Come se non bastasse, è convinzione di chi ha redatto la normativa che anche un'informazione può in qualche modo agevolare l'aggiramento di una "misura tecnologica", cosicchè è persino ostacolata **la libera diffusione e condivisione di "dati e notizie riguardanti tecniche, sperimentazioni o falle"**. Sono infatti previste censura e severe punizioni per chiunque li diffonda anche se non compie un'effettiva violazione dei diritti d'autore. Ciò chiaramente va a danno degli utenti, che perderebbero la possibilità di essere **costantemente informati sui difetti dei programmi** e a vantaggio delle aziende, che non sarebbero più obbligate a correggerli.

>> Vietato esprimersi

"Lo scenario diventa ancora più inquietante", scrive Scalas, "se si considera che le norme dell'EUCD possono essere utilizzate dai colossi dell'editoria o del software per **censurare articoli e documenti considerati scomodi**, attraverso una semplice comunicazione privata, e senza neppure dover richiedere l'intervento di un tribunale". L'EUCD concede, a chi detiene i diritti sulle opere, nuove possibilità di azione legale contro chi diffonde illecitamente materiale, ma anche e soprattutto contro gli "intermediari" (per esempio gli ISP), coloro cioè che forniscono i mezzi per pubblicare e diffondere informazioni su Internet. Agli "intermediari", in particolare, è attribuita una maggiore responsabilità e perseguibilità legale e i motivi sono chiari oltre che dichiarati: si spera infatti che, intimoriti da queste norme, essi **oscurino più rapidamente quei siti anche solo "sospettati"** di possedere materiale lesivo del diritto d'autore; e che, in caso di effettiva violazione di tale diritto, forniscano essi stessi un indennizzo adeguato a chi detiene i diritti sulle opere. Del resto gli "intermediari" hanno più risorse finanziarie rispetto ai semplici privati dai quali, anche in caso di vittoria in tribunale, non si otterrebbe forse neanche il risarcimento delle spese sostenute per le cause legali. Se tutto ciò dovesse effettivamente accadere vi sarebbe un **aumento dei costi** dei servizi offerti dagli ISP, "così da coprire i rischi che affrontano nella loro attività", e una differenziazione delle condizioni di utilizzo, con l'introduzione "di contratti più costosi che assicurano il mantenimento online del materiale pubblicato anche in caso di lamentele, e di contratti più economici privi di tali garanzie". Solo chi potrà permettersi il primo tipo di servizio avrà libertà d'espressione.

>> Vietato diffondere

In base all'EUCD, un'opera acquistata e ottenuta legalmente in rete non può essere rivenduta o ceduta a terzi **senza l'autorizzazione dell'autore o editore**, in pratica "senza il consenso o il "filtro" di particolari persone o autorità". Di conseguenza solo gli autori o editori possono rendere disponibile questo materiale, anche quando di valore storico, giornalistico o documentaristico. La nuova normativa, in pratica, ostacola la nascita di un mercato del materiale digitale "di seconda mano", che in genere favorisce una riduzione dei prezzi e quindi una maggiore circolazione del sapere; impedisce la conservazione nel tempo di materiale informativo e l'accesso a documentazione storica. Se gli autori o editori, infatti, dicessero "no" alla sua diffusione, sarebbe illegale far circolare una copia di questo materiale; se lo alterassero o modificassero, nessuno potrebbe far conoscere la versione originale senza commettere reato.

DaMe`
www.dvara.net/HK

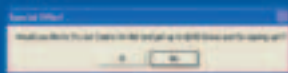
ALTRO CHE ARMONIZZAZIONE!

Appare chiaro, in conclusione, come l'EUCD incoraggi il monopolio assoluto della cultura da parte di pochi e sia finalizzata più al controllo del sapere che alla sua diffusione. Pone in primo piano soprattutto la salvaguardia dell'interesse economico dei detentori dei diritti sulle opere (più degli editori che dei reali autori), e non tutela affatto i diritti degli utenti per i quali sono invece previste nuove e maggiori limitazioni. Infine, si dimostrerebbe del tutto ignorante del principio secondo cui - citazione di Scalas - "lo sviluppo di una società aperta e colta dipende da un equilibrio tra i differenti bisogni dei suoi membri. Un'enfasi eccessiva sui diritti di alcuni individui ed istituzioni può solamente danneggiare la società dell'informazione a cui la direttiva pretende di giovare". Ma non è ancora troppo tardi! Entro il 22 dicembre 2004, la Comunità Europea esaminerà gli effetti dell'EUCD e per allora saranno presentate diverse prove dei danni che ha arrecato. Se avete davvero a cuore la libertà di espressione e la possibilità di accesso al sapere, potete ancora far sentire la vostra voce!

12_14_hj28_dial 11-06-2003 10:18 Pagina 12

PIANGE IL TELEFONO

Connessioni instabili e che non funzionano a dovere, programmi sconosciuti in esecuzione sul PC e soprattutto bollette salatissime: tutti sintomi che siete stati catturati da un dialer.

I dialer sono programmini che si scaricano da Internet e modificano le impostazioni di Accesso Remoto in Windows, in modo da stabilire una connessione con un numero telefonico a pagamento, invece che con il normale numero di accesso del provider. I costi del collegamento effettuato con un dialer è variabile, e può arrivare fino a **2,5 euro + Iva al minuto, più uno scatto alla risposta di 2 euro**. In sé, la cosa potrebbe anche non essere male, può essere utile se si vuole accedere a un contenuto o un servizio a pagamento senza usare carta di credito o senza dover sottoscrivere abbonamenti a lungo termine. L'utilizzo dei dialer potrebbe insomma essere un efficace modo per effettuare micro pagamenti su Internet. Il problema è che molti di questi fornitori di servizi a pagamento, **invece che spiegare chiaramente il funzionamento e i costi dei dialer, fanno di tutto per raggirare l'utente**, riuscendo a spillargli anche **centinaia di euro al mese** senza che se ne accorga.

Chi regala 200 dollari da giocare al casinò? Forse qualcuno che intende spillarvi almeno il doppio con la bolletta telefonica.

>> Come ti fregano

Solitamente, si incappa in un dialer quando –per scelta o perché dirottati lì da una finestra pubblicitaria– si finisce su un sito erotico, o che offre servizi di vario tipo, come loghi e suonerie per cellulari, Mp3, software… I dialer dei servizi più "seri" (se così si può dire), vengono scaricati solo dopo nostra esplicita richiesta, mostrano chiaramente qual è il prezzo della connessione, e non modificano in modo permanente il sistema.

Tra i comportamenti peggiori messi in atto dai dialer "maliziosi" troviamo:

- **download automatico** all'apertura di una pagina, senza che nemmeno l'utente abbia chiesto di scaricare alcunché.
- Uso di un messaggio di conferma simile a quello dei plug-in di Internet, **senza una chiara indicazione dei costi** di collegamento.
- I siti dicono a grandi lettere che **il download del dialer è gratuito**, ma nascondono le minuscole scritte sugli effettivi costi.
- Molto spesso, **la modifica della connessione di Accesso Remoto è permanente**. Invece di ripristinare la configurazione originale al termine della connessione, il Dialer fa in modo che –ogni volta che si effettua una normale connessione Internet– venga chiamato il numero a pagamento invece che quello del provider. In certi casi, addirittura non viene creata una nuova connessione, ma viene **modificato il numero di accesso del solito provider**, per non far venire sospetti all'utente.
- Spesso i dialer **"nascondono" il numero chiamato** nella finestra di Accesso Remoto, per non far sospettare che si tratti di un numero a pagamento.
- Il dialer si installa con **nomi insospettabili in varie cartelle di sistema**, e rimane attivo in memoria.
- In certi casi, il dialer **è in grado di reinstallarsi qualora venisse cancellato** il file principale (come molti virus).

COME EVITARE DI FARSI INCASTRARE

Un dialer cerca sempre di scaricarsi e avviarsi senza far accorgere di nulla il navigatore. Per fare ciò, utilizzano vari trucchi che bene o male si basano su caratteristiche molto rischiose di Internet Explorer e di Windows. Chi usa Mac OS o Linux è quindi tranquillo (finché qualcuno non deciderà di scrivere dialer anche per questi sistemi…).
Se usate Windows e non volete rinunciare a Internet Explorer (beh, ve le cercate, eh?), prendete come minimo queste precauzioni:

• Se state seguendo un link che secondo voi dovrebbe portare a una pagina o un'immagine, e non a un programma eseguibile, e compare una finestra di dialogo che chiede se scaricare o eseguire un programma, fate clic su annulla.
• Se compare una finestra di dialogo che vi chiede di scaricare e installare un Plug-In, e non siete più che sicuri dell'affidabilità del sito e del certificato, fate clic su Annulla. In molti si fanno rassicurare dal fatto che viene comunque visualizzato un certificato di certificazione, anche se è emesso da una società praticamente sconosciuta.

Inoltre si narra di alcuni dialer che, come molti virus e trojan, si fondono con programmi eseguibili e processi di sistema (join) per essere lanciati a ogni avvio di Windows rimanendo completamente invisibili all'utente. Di questo tipo, fortunatamente, noi non ne abbiamo mai visti, ma sono sicuramente una minaccia da tenere in considerazione.

>> Dove si infilano

Innanzi tutto, viene ovviamente creata una nuova Connessione di Accesso Remoto (**c:\Pannello_di_controllo\opzioni_internet_explorer\CONNESSIONI**), o viene modificata quella già presente. In certi casi, viene creato un collegamento sulla Scrivania o nella barra delle applicazioni; questo probabilmente per ingannare una volta di più gli utenti meno esperti, che cancellando il collegamento pensano di aver rimosso il programma, che invece rimane attivo e continua a succhiare soldi. Il vero programma principale rimane però nascosto in una qualche cartella, che può essere annidata ovunque nel sistema (**c:\windows\Programmi**, **c:\Documenti**, **c:\Windows\System**…). Questo programma ha il compito di avviarsi periodicamente (o all'avvio del sistema), verificare se le impostazioni di Accesso Remoto sono state ripristinate alle loro originali condizioni, e in questo caso modificarle ancora una volta, inserendo il numero a pagamento. Il programma principale potrebbe anche rimanere sempre attivo in memoria, agendo come un virus, che non può essere cancellato definitivamente se non avviando il sistema da una partizione diversa, o da floppy o CD.

>> Come trovarli

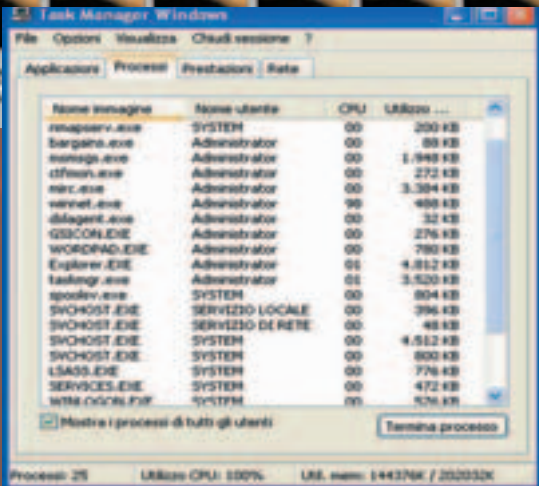
Se vi siete già beccati un dialer "di quelli bastardi", che si insinuano nei meandri del sistema per rimanerci più che possono, come prima cosa dovrete trovare tutti i riferimenti al dialer. Dovete prendervi un po' di tempo, ed esaminare con calma tutte le possibili posizioni in cui il dialer può essersi installato e configurato per un avvio automatico alla partenza del sistema. **Non mettetevi a cancellare i file e le impostazioni mano a mano che le trovate**: limitatevi a prendere nota su un foglietto, per poi cancellarle tutte quante insieme, possibilmente avviando da un floppy di MS-DOS, per essere sicuri che il dialer presente in memoria non annulli immediatamente ogni vostra modifica.
È bene **controllare tutte le posizioni che vi suggeriamo**, evitando di fermarsi al primo successo: molti dialer, per "stare tranquilli", installano più di una copia del programma, ciascuna impostata per partire automaticamente da diverse posizioni.
Le posizioni del sistema da cui può essere impostata l'esecuzione automatica di un programma (o in cui possono comparire degli indizi) sono: la cartella Esecuzione Automatica, il Registro di Windows, il file Win.ini, il file System.ini, i Servizi di sistema, e i file di Avvio. Fate attenzione a una cosa: la stragrande maggioranza dei servizi e dei programmi registrati in queste posizioni **sono assolutamente innocenti**, e anzi sono necessari al funzionamento di Windows. **Evitate di cancellare file o impostazioni a casaccio**, "giusto per stare tranquilli…": rischiereste di rendere inutilizzabile il vostro computer.

>> Programmi residenti in memoria

Come prima cosa, verifichiamo se per caso un programma malizioso è già attivo in memoria, cosa che vanificherebbe ogni tentativo di pulizia. Premendo una sola volta **Control+Alt+Canc** compare una lista dei processi attivi noti a Windows. Potrebbero benissimo essercene degli altri, che non compaiono in questo elenco, ma è già qualcosa. Prima di ogni altra operazione, bisogna terminare i programmi che non vi risulta debbano essere attivi. Per evitare confusioni, è meglio **chiudere manualmente qualsiasi programma, utility o servizio attivo** (firewall, antivirus, programmi di messaggistica eccetera).

>> Programmi lanciati all'avvio

Per vedere tutte le applicazioni poste in esecuzione automatica (non provate da Start/Programmi/Esecuzione Automatica perché non trovereste molto). Bisogna cliccare su **Start**, poi **Esegui**, e di-

Pensavate di vedere un'immagine e vi ritrovate un programma? Non apritelo!

Dal Task Manager di Windows, che compare premendo una volta Control+Alt+Canc, si possono vedere i programmi attualmente in esecuzione: potrebbe esserci il programma di un dialer.

SE IL DANNO C'È GIÀ STATO...

Se già avete ricevuto una bolletta salata per colpa di un dialer, potete contestarla. L'associazione di consumatori Codacons ha pubblicato sul proprio sito un articolo a riguardo; c'è qualche imprecisione tecnica qua e la, ma dal punto di vista dei diritti, sanno il fatto loro. In particolare, il Codacons suggerisce di:

- Non pagare per intero la bolletta, ma solo la parte di telefonate che si riconosce;
- Sporgere denuncia alla Polizia Postale, scaricando il modulo che si trova all'indirizzo www.codacons.it/modelli/stop709.html
- Mandare al gestore telefonico copia della denuncia alla Polizia Postale, e copia del versamento parziale.
- Rivolgersi al Codacons, i cui legali offrono assistenza per evitare di pagare cifre non dovute.

gitare il comando: **msconfig**. Il programma esiste in tutti i sistemi operativi di casa Microsoft. Apparirà una schermata con varie pagine. Cerchiamo la pagina **Esecuzione Automatica** (win95/98/nt/Me) o **Avvio** (Win2000/XP), dovrebbe essere l'ultima. Da questa pagina vediamo tutto ciò che noi abbiamo in esecuzione automatica, e anche il "Full Path" cioè il percorso esatto dei nostri File. In Windows XP viene anche visualizzata la chiave di registro nella quale il dialer è impostato; con le versioni precedenti di Windows, abbiamo ottenuto almeno il nome dell'eseguibile, e quindi possiamo cercare nel registro le chiavi in cui compare, per poterle rimuovere.
Ammettiamo MSconfig ci dica che il dialer si trovi in **c:\Program Files\Dialer\Nomedialer.exe**, Andiamo nella cartella in questione e cancelliamo il file oppure l'intera cartella, se siamo sicuri che non contenga file di sistema. Dopodiché, deselezioniamo il valore del dialer dalla lista dei programmi eseguiti all'avvio. Attenzione… in Windows 2000 e XP quando deselezionate qualche valore, si cambiano le configurazioni di Avvio in una pagina precedente sempre di MSconfig, e il sistema operativo passa così da **Avvio automatico** ad **Avvio manuale e selettivo**; bisogna quindi ripristinare l'impostazione una volta finito tutto.
Controllate anche le voci presenti in **Win.ini** e **System.ini** (sempre in MSconfig), e agite come in precedenza: leggete e annotate la posizione esatta del programma sospetto (es: **c:\windows\dialer**), deselezionate il programma dall'elenco e cancellate l'eseguibile dal disco.

>> Il registro di sistema

MSconfig non fa altro che mostrare in modo più simpatico le vere impostazioni, che risiedono in file di sistema oppure nel registro, come appunto le impostazioni sui programmi da lanciare all'avvio.
Per modificare il registro bisogna usare il programma regedit, che si può lanciare dal menu **Start/Esegui**, digitando appunto **regedit** e premendo **Invio**. Compare la struttura ad albero del registro, nella quale cercare le chiavi giuste, facendo clic sul **[+]** per aprire le cartelle, come se si trattasse di directory del disco. I programmi eseguiti automaticamente all'avvio del sistema sono nelle chiavi:

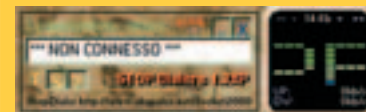
```
HKEY_CURRENT_USER/SOFTWARE/Microsoft/Windows/CurrentVersion/RUN
HKEY_LOCAL_MACHINE/SOFTWARE/Microsoft/Windows/CurrentVersion/RUN
```

Selezionate la voce con il nome dell'eseguibile del dialer, e premete **Canc**.
Il dialer potrebbe anche aver registrato altre chiavi, che conviene rimuovere. Sempre in **regedit**, fate clic su **Modifica**, poi su **Trova**, e inserite il nome dell'eseguibile trovato in **MSconfig** o nel **Task Manager**. Eliminate anche quelle chiavi.

>> Facciamo una verifica

Dopo aver eliminato tutto quanto, provate a riavviare il sistema e a ricontrollare tutte le posizioni in cui avevate trovato il dialer: cartella con l'eseguibile, Task Manager, MSconfig, Registro di sistema… **Se non compare nulla, siamo a cavallo**: avete estirpato il dialer. Se invece il bastardo è ritornato, **probabilmente è rimasto un programma residente in memoria che ha annullato le nostre modifiche**. Non rimane che ripartire da un dischetto sicuro, ed eliminare manualmente l'eseguibile e i file relativi (senza toccare i file di sistema). **Probabilmente, al successivo riavvio, compariranno degli errori**, perché Windows cercherà di eseguire nuovamente il dialer all'avvio, ma non lo troverà più. Ripetete i passi relativi al Registro e a MSConfig per eliminare ogni riferimento al dialer, e gli errori non dovrebbero più presentarsi.

Hanno collaborato:
NeOs ed **Emanuele Gentili** (0x6D6362)

PREVENIRE È SEMPRE MEGLIO...

Visto che rimuovere un dialer già installato è peggio che cercare di staccare un calciatore da una velina, è meglio evitare il problema alla radice. Ecco come:

- Telefonare al 187 e chiedere di disabilitare dalla propria linea tutti i numeri a pagamento.
- Usare un programma che blocca i dialer, come Dialer Control (www.dialercontrol.de) o Stop Dialer (www.akapulce.net/socket2000/stopdialer.asp, in italiano)
- In Internet Explorer, andate su Strumenti/Opzioni Internet/Protezione, e impostate il livello di protezione su Medio o su Alto.

Perlomeno qualcuno invita a leggere le condizioni d'uso prima di avviare il programma.

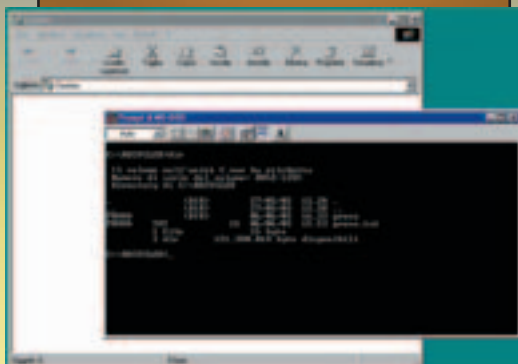
NEWBIE

NASCOSTI NEL CESTINO

File e documenti riservati possono essere nascosti alla vista degli utenti di Windows semplicemente spostandoli nel Cestino con qualche colpo di MS-DOS.

COMANDI DOS

del nomefile
Elimina uno o più file (per esempio "del file.zip" elimina file.zip)
copy nomefile nuovopercorso\nomefile
Copia un file in un'altra cartella (per esempio "copy file.zip c:\documenti" copia file.zip in c:\documenti).
cd nomedirectory o percorso
Cambia directory (o senza nessun argomento visualizza la directory in cui siamo). cd.. risale di una gerarchia l'albero delle directory.
move nomefile nuovopercorso\nomefile
Sposta un file da una directory a un'altra. Se si omette il secondo nomefile, il file avrà lo stesso nome.
xcopy nomedirectory nuovopercorso\nomedirectory
Copia un'intera directory e tutto il suo contenuto in una diversa posizione.
dir
Visualizza il contenuto di una directory

Il cestino di Windows è una speciale cartella di sistema (nascosta), che ha la funzione di contenere i file da cancellare. Questa cartella ha **alcune caratteristiche particolari** e non standard, che cercheremo di sfruttare in questo articolo per nascondere file e informazioni.
Ogni unità (ogni disco) ha un cestino, ossia ha una cartella contenenti i file da eliminare di quell'unità. Questa cartella, chiamata "**recycled**", si trova nella directory root dell'unità (C:\, D:\ eccetera) e non si può eliminare.

La finestra del Cestino è vuota, ma da MS-DOS si possono vedere il file prova.txt e la directory Prova.

>> Il nucleo della faccenda

Solitamente, quando da Windows facciamo doppio clic sull'icona di una cartella, ce ne viene mostrato il contenuto in una finestra. A prima vista, **parrebbe che lo stesso avvenga anche con il Cestino**, ma **le cose non stanno esattamente così**. Il Cestino infatti mostra tutti i file che sono stati spostati dall'interfaccia di Windows, ma **non quelli che sono stati copiati manualmente, da MS-DOS**, nella directory Recycled. Cominciate a intuire qualcosa? Bene.
Il punto è questo: se, dal prompt di MS-DOS, spostate il file prova.txt nella directory recycled, con un comando tipo:

```
copy prova.txt
\recycled\prova.txt
```

Il risultato sarà che il file di testo sarà visibile solo dal prompt di MS-DOS, (con dir c:\recycled), ma non da Windows.
E il bello è che, essendo invisibile al sistema, il file rimarrà in quella posizione anche se svuotate il Cestino con l'apposito comando di Windows. Per eliminarlo bisognerà infatti utilizzare il comando del, sempre dal prompt di MS-DOS.
Per ripristinare il file (sempre sotto DOS) basta entrare in recycled (cd recycled), copiare il file da un'altra parte (copy file.xxx c:\) ed eliminarlo da lì (del file.xxx), oppure fare tutto in un'unica operazione usando il comando move.

>> Considerazioni

Ovviamente, i file sono nascosti alla vista, ma perfettamente accessibili a chiunque venga in mente di curiosare nel cestino dal prompt di MS-DOS. Può trarre in inganno qualche capoufficio, o qualche familiare, ma chiunque con un minimo di capacità tecnica (o anche chiunque legga questo numero di HJ) può facilmente svelare i vostri file "segreti". Evitate anche di dimenticarvi nel Cestino file molto ingombranti, che occuperebbero inutilmente molto spazio.

nortoz

UNO SCRIPT CHE FA TUTTO

Questo piccolo script Batch permette di effettuare in un'unica operazione la copia nel cestino e la cancellazione di un file dalla sua precedente posizione. Scrivete il tutto in un editor di testo (testo, non Word, non Rtf, non altro), salvatelo col nome hide_this.bat (o quello_che_volete.bat) e lanciatelo dal prompt di MS-DOS semplicemente digitando il nome del file e premendo Invio.

```
@echo off
if "%1"=="" goto :print
copy %1 c:\recycled>nul
del %1
goto :end

:print
echo ———————————————————-
echo Usage:
echo hide_this.bat file_da_nascondere
echo ———————————————————-
:end
```

16_19_hj28_tel 11-06-2003 10:25 Pagina 16

TELNET E I SUOI 1000 USI

Con telnet si fanno attività serissime, come controllare un server remoto, ma anche cose divertenti, come giocare a scacchi o... guardarsi Guerre Stellari.

Telnet è un protocollo utilizzato per scambiare messaggi di testo con un server remoto; questi "messaggi" possono essere informazioni oppure comandi, che devono essere interpretati ed eseguiti dal server (o da un programma che giri su di esso).
Solitamente, una installazione di Windows comprende già due diversi programmi che possono essere usati per stabilire connessioni Telnet: uno è **HyperTerminal**, che si trova tra gli strumenti di comunicazione, e l'altro è un **programma a linea di comando**, che può essere lanciato direttamente dal prompt di MS-DOS. Gli utenti che utilizzano Windows 98 lo possono trovare in c:\windows (c:\windows\System 32 per gli utenti che usano Xp).
Quindi andate su **Start/Esegui**, digitate **Telnet** e premete **Invio**.
Nel corso di questo articolo faremo riferimento al Telnet installato su Windows 98 (tranne per l'aspetto grafico quello che faremo con il Telnet di Windows 98, sarà valido anche per tutti gli altri Telnet).

>> Impostare le preferenze

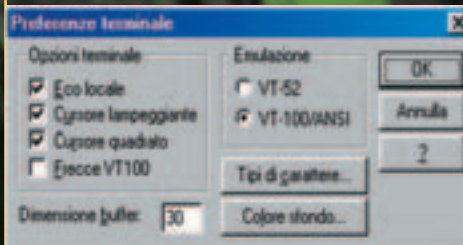



Figura 1: le preferenze di Telnet.

Settiamo il nostro terminale Telnet secondo i nostri gusti.
Andiamo sul menù a tendina **Terminale** e quindi su **Preferenze (figura 1)**:
Oltre a impostare l'aspetto grafico del terminale (tipo di carattere, colore e sfondo) è importante selezionare **Eco locale** (in modo da visualizzare quello che noi digitiamo) e come emulazione **VT-100/ANSI** (che è lo standard più comune).
Inoltre se volete aumentare l'ampiezza (intesa come numero di righe) del vostro terminale Telnet, aumentate la **Dimensione buffer** (di default è 25).
Prima di connetterci fisicamente al server potrebbe essere opportuno registrare tutto quello che facciamo durante la nostra sessione Telnet; quindi andiamo su **Terminale** e poi su **Inizia registrazione**; ci verrà quindi chiesto di scegliere la directory e il nome del file (*.log) dove vogliamo memorizzare il nostro dialogo con il computer remoto.

>> Prima connessione

A questo punto siamo pronti per realizzare la nostra prima connessione tramite Telnet. Dobbiamo solamente decidere a quale servizio vogliamo connetterci (posta, BBS, accesso a database, tempo libero…)

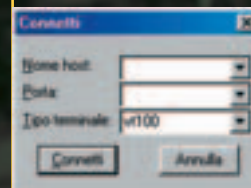



Figura 2: la finestra di connessione.

Clicchiamo su **Connetti** e poi su **Sistema remoto**; ci verrà presentata la finestra mostrata in figura 2:
Nella casella **Nome host** introduciamo il nome del server al quale ci vogliamo connettere (si può introdurre in alternativa l'indirizzo IP; basta fare un semplice ping per ricavare l'indirizzo

16_19_hj28_tel 11-06-2003 10:25 Pagina 17

Su Mac OS X, telnet è accessibile come programma da linea di comando, usando il Terminale.

IP dal nome host).
Gli utenti che usano il Telnet di Xp o di Linux, debbono digitare al prompt del Telnet il seguente comando:

```
open nomehost porta
```

Per quanto riguarda la porta (di default è la porta 23, standard per Telnet) dobbiamo inserire la porta del servizio a cui vogliamo accedere.
Tra le porte principali troviamo:

```
13    DAYTIME
21    FTP
23    TELNET
25    SMTP
43    WHOIS
79    FINGER
80    HTTP
110   POP3
```

Vediamo alcuni semplici utilizzi di Telnet. Nel testo che segue, le righe in rosso sono quelle che bisogna scrivere sul client, mentre quelle in blu sono le risposte del server.

>> Spedire e-mail (vere o false)

Come nome host scegliamo un server che permetta l'invio della posta (es: mail.libero.it), come porta scegliamo ovviamente la 25 (SMTP) e clicchiamo su Connetti. In generale vi consiglio di scegliere il vostro provider perché altrimenti non è garantito l'invio della e-mail.
Siamo quindi connessi al server di posta di Libero (e viene visualizzata la seguente linea):

220 smtp2.libero.it ESMTP Service (7.0.012) ready

Digitando **HELP** comparirà una lista dei comandi accettati; con **HELP nomecomando** abbiamo ulteriori dettagli sul determinato comando.
Dobbiamo ora impartire le giuste istruzioni per spedire l'e-mail.

Iniziamo con il salutare il server identificandoci (si potrebbe mettere un qualsiasi nome, ma è meglio mettere il nome del dominio; questo perché il nome digitato qui va a finire negli headers della e-mail):

HELO libero.it
250 smtp2.libero.it

Scriviamo il mittente della e-mail:

MAIL FROM: <bobo.vieri@cannonieri.it>
250 MAIL FROM:<bobo.vieri@cannonieri.it> OK

Scriviamo il destinatario della e-mail:

RCPT TO: <robinhood.sherwood@libero.it>
250 RCPT TO: <robinhood.sherwood@libero.it> OK

Diciamo al server di voler iniziare a scrivere il corpo della e-mail:

DATA
354 Start mail input; end with <CRLF>.<CRLF>

Digitiamo il corpo della e-mail (con le relative intestazioni):

From: "Christian Vieri" <bobo.vieri@cannonieri.it>
To: "Robin Hood" <robinhood.sherwood@libero.it>
Date: Sun, 03 Jun 2003 21:47:15 +0100

(la data può anche essere omessa, il server provvederà da solo ad aggiungerla)

Subject: Prima e-mail con Telnet

Quando è che ci vediamo per fare una partita di calcetto?
Ciao a presto.

(con il punto finale, su una riga vuota, il server capisce che abbiamo chiuso la nostra e-mail)

<3E9BEBC30106F438> Mail accepted

L'e-mail è stata accettata, abbiamo finito e quindi digitiamo:

QUIT
221 smtp2.libero.it QUIT

>> Leggere le e-mail

Questa volta ci dobbiamo collegare con il nostro servizio di posta elettronica (esempio popmail.libero.it) alla porta

FAKE MAIL CON OUTLOOK EXPRESS

Naturalmente si possono mandare e-mail burla anche attraverso Outlook Express senza passare per Telnet; infatti basta creare un account finto (Strumenti Account Posta elettronica Aggiungi….).
Inseriamo il nome fasullo e nel campo SMTP mettiamo un server valido; il POP3 naturalmente può essere uno qualsiasi (tanto dobbiamo spedire le e-mail e non riceverle!).
Attenzione: in teoria inviare e-mail con falso nome è reato (perché si sta usando l'identità di un'altra persona), ma non è assolutamente reato fare uno scherzetto al nostro carissimo amico che è un grande ammiratore di una certa attrice e non vede l'ora di ricevere un invito a cena!

SVAGO E DIVERTIMENTO

Se siamo alla ricerca di un luogo dove parlare e scambiare opinioni possiamo collegarci a bbs.cittadellabbs.it e come porta specificare 4001. Nei settaggi del Telnet spuntate eco locale, altrimenti le lettere che digitate verranno visualizzate doppie!

Dopo alcuni messaggi di presentazione viene fornita la lista dei comandi.

Vogliamo fare una partita a scacchi on-line? Possiamo allora collegarci ad un server FICS inserendo come nome host freechess.org e come numero di porta la 23 (Telnet) ecco il risultato:

Naturalmente vi potete anche collegare normalmente con il vostro browser all'indirizzo www.freechess.org e giocare a scacchi con un interfaccia grafica.

110 (servizio pop3).

Appena collegati al servizio, vediamo che la connessione è andata a buon fine perché il server si presenta ed è pronto a ricevere i nostri comandi:

+OK POP3 PROXY server ready (6.5.001) <E3F4A1A7A5F95557E4137381BF0E4E6300D3E3A5@pop1.libero.it>

A questo punto iniziamo a dare i comandi di identificazione user e password:

user robinhood.sherwood
+OK Password required
pass lamiapassword
+OK 6 messages

Il server mi ha riconosciuto e mi dice che ho 6 messaggi nella mia casella di posta elettronica.
Vediamo alcuni comandi, cominciando con stat, che serve per vedere il numero dei messaggi e la loro dimensione complessiva in bytes:

stat
+OK 6 80184

Per avere una lista dei messaggi con la rispettiva dimensione invece si usa list:

list
+OK
1 4069
2 5497
3 3647
4 18155
5 3824
6 44992
.

Per visualizzare il primo messaggio dobbiamo usare:

retr 1
+OK 4069 bytes
Return-Path: <newsletters@intelligiochi.com>
Received: from smtp5.libero.it (193.70.192.55) by ......

Molto probabilmente il messaggio è troppo lungo e non entra nel vostro terminale Telnet (ma se avete attivato il log della connessione, tutto il contenuto della e-mail è stato salvato nel file log), tuttavia per leggere l'email in maniera più agevole si può ricorrere al comando top, che ha bisogno di due parametri: il primo numero indica il numero del messaggio, mentre il secondo indica il numero di righe da visualizzare. Fate attenzione al fatto che tutti gli headers (intestazioni) della e-mail contano come una riga.

top 1 10

Se invece volessimo cancellare un messaggio basta ricorrere a:

dele 1
+OK message marked for deletion

Alcuni pazzi hanno riprodotto l'intero film di Star Wars in caratteri Ascii animati: si può vedere lo spettacolo collegandosi con Telnet all'indirizzo towel.blinkenlights.nl (non sempre è in funzione).

Come si può vedere, il messaggio non è stato ancora cancellato fisicamente ma è stato marcato per essere cancellato, alla fine della connessione. Se ci siamo sbagliati, possiamo quindi tornare indietro con il comando rset, che fa dimenticare tutte le cancellazioni marcate in precedenza nel corso della sessione.:

rset
+OK

Quando abbiamo finito di interrogare il server chiudiamo la connessione tramite:

quit
+OK POP3 server closing connection

>> Orario ufficiale

Se vogliamo sapere l'orario ufficiale possiamo collegarci con l'Istituto Galileo Ferraris; come nome host mettiamo time.ien.it e come porta ovviamente la 13 (ossia DayTime).

NEWBIE

Ottenere le RFC (Request for Comments)
Le RFC costituiscono il punto di riferimento degli standard di comunicazione per Internet. Di seguito trovate le specifiche delle RFC che interessano i principali protocolli; si possono prelevare dal sito www.rfc-editor.org

SMTP (Simple Mail Transfer Protocol) RFC 821
POP3 (Post Office Protocol) RFC 1939
FTP (File Transfer Protocol) RFC 959
TFTP (Trivial File Transfer Protocol) RFC 1350
HTTP (HyperText Transfer Protocol) RFC 2068
TELNET RFC 854 RFC 855
TCP (Trasmission Control Protocol) RFC 793
IP (Internet Protocol) RFC 791 RFC 1883
UDP (User Datagram Protocol) RFC 768

Il server dopo averci fornito la data e l'ora esatte, ci sconnetterà automaticamente:

```
Sun Jun 1 17:51:30 2003
```

>> Interroghiamo un server WHOIS

Vogliamo ottenere ad esempio informazioni sul dominio hackerjournal.it
Quindi come host selezioniamo whois.nic.it e quindi come porta la 43 (servizio whois).
Connessi al server lo possiamo interrogare digitando semplicemente

```
hackerjournal.it
```

Qui di seguito parte del risultato ottenuto:

```
domain:       hackerjournal.it
x400-domain:  c=it; admd=0; prmd
              hackerjournal;
org:          Sprea Editori s.r.l.
org-unit:     Internet Service Provider
descr:        Via Torino, 51
descr:        20063 Cernusco s/N (MI)
......
nserver:      213.198.155.21 ns0.i-m-c.it
......
created:      20020506
expire:       20040517
......
```

>> Consultare un newsgroup

Se vogliamo ad esempio consultare un newsgroup possiamo inserire come host news.libero.it e come porta inseriamo la **119** (si noti che solitamente il server news di un provider accetta connessioni solo se provengono da propri utenti).
A questo punto digitando help abbiamo un quadro dei comandi disponibili.
Ad esempio con **list** (visualizziamo tutta la lista dei newsgroup); con **listgroup nome.del.newsgroup** visualizziamo il numero di articoli presenti all'interno del newsgroup.
Con il comando **article numero** leggiamo l'articolo selezionato.
Al solito con il comando **quit** chiudiamo la connessione con il server delle news.

>> Altri client Telnet

Qualora il Telnet allegato a Windows vi risulti limitativo potete provare con altri client (vedi box).
Se vogliamo un client semplice da utilizzare che non sia dispersivo nei vari settaggi possiamo utilizzare **KevTerm**; questo piccolo programma freeware costituisce già un miglioramento rispetto al client classico di Windows, in quanto l'input può essere digitato su una linea di comando separata e quindi quando siamo sicuri della sintassi del comando lo possiamo inviare al computer remoto. Con il client di Windows, infatti, appena digitiamo un carattere questo viene spedito al terminale remoto, impedendoci di correggere eventuali errori di digitazione.
Inoltre è possibile creare una libreria di comandi di più frequente uso (macro) che possono essere velocemente richiamati con una combinazione opportuna di tasti velocizzando in maniera non indifferente il colloquio con il terminale remoto.
Un po' più complesso e dispersivo per quanto riguarda i settaggi risulta **Putty**, da molti indicato come il miglior client freeware in circolazione; una delle sue caratteristiche più importanti è quella di supportare anche il più sicuro protocollo SSH (oltre al telnet).
Se vogliamo client con maggiori funzionalità dobbiamo rivolgerci a dei trialware (piene funzionalità ma solo per 30 giorni) come **CRT**, **KoalaTerm** o **Tn3270 PLUS**.
Tutti quanti più o meno hanno le stesse funzionalità: permettono di salvare i parametri di ogni singola connessione (interfaccia grafica, macro……), estrema flessibilità nella gestione dello schermo (zoom delle scritte con un semplice click), immissione dei comandi diretta o tramite linea di comando (tipo chat), stampa della sessione effettuata, ricerca delle parole all'interno della sessione.
Particolarità di **Tn3270 PLUS** è quella di avere al suo interno una serie di strumenti quali ping, finger, whois, checkmail (POP3) e DNS lookup.
Inoltre è possibile creare script e macro in modo da sveltire le operazioni; per tale obiettivo sembra particolarmente adatto per la semplicità di utilizzo **KoalaTerm** che permette la realizzazione di macro (richiamabile con un semplice clic su di un bottone) attraverso una registrazione in tempo reale dei comandi impartiti al terminale remoto.
Quali di questi 3 sia effettivamente il migliore dipende dai vostri gusti e dalle vostre singole esigenze.

>>--Robin-->

DOVE SCARICARE GLI ALTRI CLIENT TELNET

KevTerm 2.02 [Freeware]
http://www.geocities.com/SiliconValley/Network/1027/

PuTTY 0.53b [Freeware]
http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

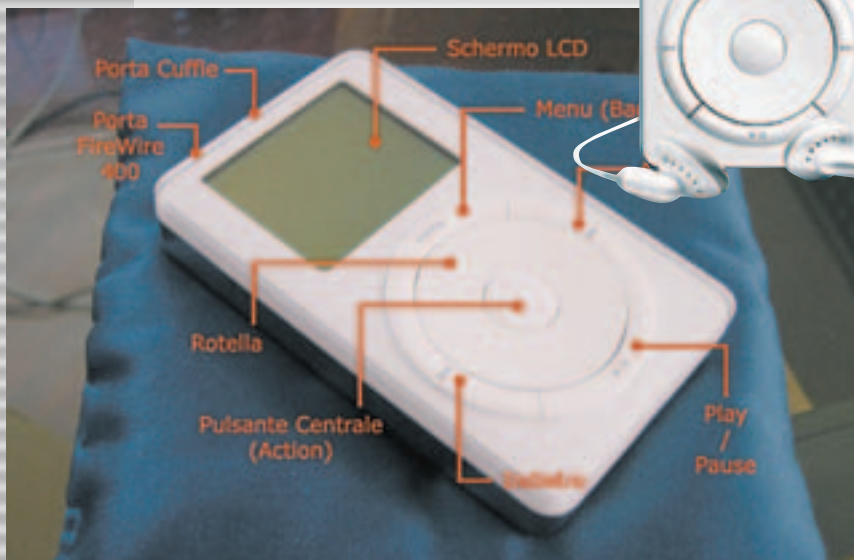
KoalaTerm 4.1 [Trialware 30 gg.]
http://www.foxitsoftware.com/mkt/mkt.zip

Tn3270 PLUS 2.3 [Trialware 30 gg.]
http://www.sdisw.com/

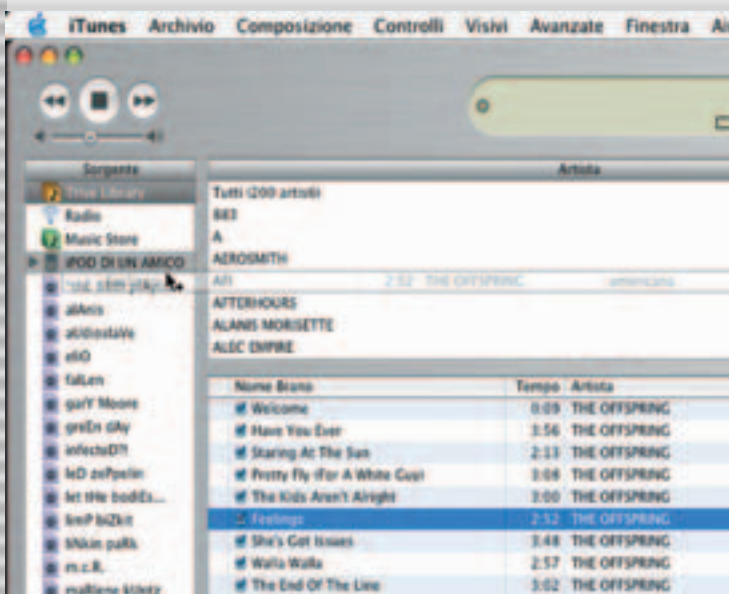
CRT 4.0.6 [Trialware 30 gg.]
http://www.vandyke.com/download/crt/index.html

20_22_hj28_pod 11-06-2003 10:28 Pagina 20

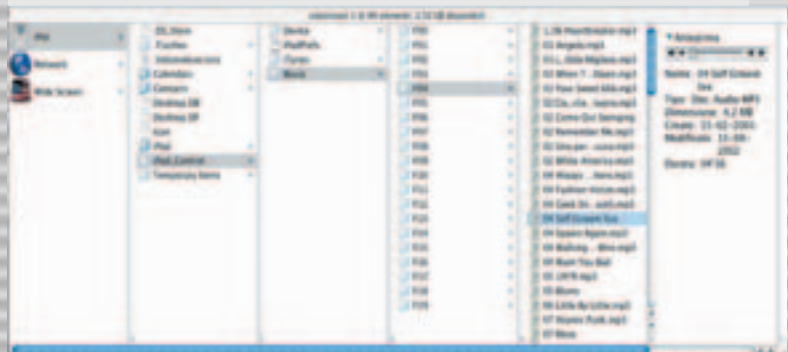
I Hack the

Firmware, modalità nascoste, utilizzo su piattaforme non supportate e persino installazione di Linux: nel lettore Mp3 di Apple c'è molto più di quello che appare.

Schema generale dell'iPod.

>> Copiare file senza limiti

Grazie a iTunes (o a Music Matchbox su Windows) è possibile organizzare in maniera veloce la musica sul proprio iPod. Abbiamo due possibilità: o lasciar fare ogni cosa al computer (in questo caso la nostra collezione di Mp3 sarà riportata uguale identica sul lettore) o gestire manualmente il tutto (ciò richiederà lo spostamento manuale di Mp3 e playlist). Questa ultima scelta ci permetterà di collegare l'iPod di un amico e trasferirgli qualche Mp3 o playlist; ricordiamoci solo che **esso sarà sincronizzato con un altra libreria** e quindi dovremo rispondere "NO" nel caso iTunes ci chiedesse di sincronizzarlo con la nostra.

Il contenuto dell'iPod di un amico come viene visualizzato da iTunes. Da qui si possono copiare file dal Mac sull'iPod, ma non viceversa.

Funzione molto interessante è l'**abilitazione di iPod come disco FireWire**, che permette un trasferimento velocissimo di file verso Mac con OS X.

E per trasferire musica dall'iPod al computer? La cosa **ufficialmente non è supportata da Apple** (per evitare duplicazioni abusive degli Mp3), ma è nostro diritto backuppare gli Mp3 che abbiamo sul lettore. Si può certamente provare ad **analizzare il contenuto di iPod**: il primo passo è attivare il lettore come disco FireWire e poi "obbligare" il sistema operativo a **visualizzare i file nascosti**. In Mac OS X possiamo utilizzare il Terminale (ed in particolare il comando **ls -a**) oppure, più comodamente, un'applicazione che ci permetta di visualizzare i file nascosti di default: **TinkerTool** fa al caso nostro (www.bresink.de/osx/TinkerTool2.html). Sotto Windows, più semplicemente, aprite iPod da **Risorse del Computer**, selezionate dal menu **Strumenti** la voce **Opzioni cartella**, quindi fate clic sulla linguetta **Visualizzazione** e scegliete **Visualizza cartelle e file nascosti**. Al di là del sistema operativo utilizzato, dobbiamo aprire la cartella **iPod_Control**, la quale contiene **Music Folder**. Questa, a sua volta, ha al suo interno 19 sottocartelle nominate F01, F02 eccetera.

L'albero delle directory interne all'iPod.

Gli MP3 sono al loro interno: non vi rimane che agire di drag&drop. Questo metodo ci permette di copiare gli Mp3, ma **non di poterli vedere organizzati per nome o artista**; a questo scopo si può usare un programma freeware come PodUtil (vedi riquadro).

20_22_hj28_pod 11-06-2003 10:29 Pagina 21

SOLO PER MAC? MA NO...

E per Windows e Linux? Riguardo Windows (ma il discorso vale anche per Mac se le applicazioni che vi ho indicato non vi soddisfacessero) un ottimo punto di partenza è www.versiontracker.com su cui potrete effettuare una ricerca con argomento "iPod" e trovare molti freeware e shareware interessanti. Vi consiglio, per la gestione di MP3 e playlist, XPlay o EphPod che non sono niente male. Invece, per quanto riguarda programmi come TextPod e iSync, i relativi "corrispondenti" Windows possono essere considerati iText e iPodSync. Per la gestione dei soli contatti, un eccellente software è bPod.
Per quanto riguarda GNU/Linux, è possibile sia usare l'iPod collegandolo a un PC che usi il sistema del pinguino (www.cs.duke.edu/~geha/ipod/, meglio avere una RedHat recente, per il supporto firewire), sia installare una particolare versione di Linux sull'iPod stesso (http://ipod-linux.sourceforge.net)!

>> Funzioni nascoste

In questo articolo farò riferimento alla versione del software 1.2 (la più diffusa). L'OS dell'iPod è molto facile da usare anche se talvolta può risultare instabile: in caso di crash, per riavviare forzatamente il lettore, è necessario **premere contemporaneamente,** fino a che non compaia la mela mangiucchiata, i tasti **Menu** e **Play**. Ipotizziamo che il nostro iPod abbia un qualche problema; **prima di mandarlo in assistenza** (dove starebbe settimane e settimane) possiamo provare a fare ciò che sicuramente farebbero anche in un laboratorio specializzato: **eseguire i test per controllare l'hardware**. Per verificare il corretto funzionamento del disco rigido si può avviare la verifica del disco. Ecco come fare: durante il riavvio forzato è necessario premere **Avanti**, **Indietro**, **Action** e **Play**: comparirà un'iconcina animata e dopo diversi minuti ci verrà comunicato l'esito del test. Per avviare altri test, invece, si deve entrare nella modalità test: durante il riavvio forzato è necessario premere **Avanti**, **Indietro** e **Action**. Ci si troverà davanti una lista di 16 test, ognuno caratterizzato da una lettera. Analizziamoli:

A. 5 IN 1: esegue tutti i test dalla J alla N.
B. RESET: ripristina il lettore.
C. KEY: verifica il funzionamento dei comandi: si hanno 5 secondi per premere tutti i tasti.
D. AUDIO: controlla il subsystem audio. Provatelo con le cuffie...
E. REMOTE: verifica il funzionamento dei comandi remoti.
F. FIREWIRE: controlla il bus FireWire.
G. SLEEP: attiva la modalità "sleep".
H. A2D: verifica il corretto voltaggio.
I. OPTO CNT: descrive i movimenti della rotella in codice esadecimale.
J. LCM: controlla il display.
K. RTC: verifica "Real Time Clock".
L. SDRAM: controlla la memoria RAM.
M. FLASH: controlla la memoria ROM.
N. OTPO (o WHEEL A2D): funziona solo su alcuni iPod e verifica alcune funzioni del pulsante Action.
O. HDD SCAN: verifica il disco rigido.
P. RUN IN: esegue in loop i test dei chipset.

Attenzione: in questa modalità la rotella non funziona. Usate Avanti, Indietro e Action per muovervi. Per uscire è necessario riavviare forzatamente.

Anche l'iPod ha bisogno di pulizia; ecco come fare nel caso la rotella andasse un po' a scatti.

>> Smontare iPod

Con un po' di **attenzione e sangue freddo** si può andare a curiosare nei meandri più nascosti dell'hardware di iPod senza fare danni. Dopo molti mesi di utilizzo la rotella potrebbe risulta-

LINK UTILI

www.apple.com/ipod
Homepage ufficiale iPod.

www.ipodlounge.com
Un vero punto di riferimento.

www.versiontracker.com
Qui trovate tutto il software citato nell'articolo.

APPLICAZIONI E UTILITY PER MAC

PodUtil
www.kennettnet.co.uk/software/podutil.htm
Visualizza il contenuto di un iPod per artista o titolo, come iTunes, ma permette anche di copiare Mp3 dall'iPod al Mac.

PodText
Permette di trasferire note e testi sull'iPod, spezzettando i più lunghi.
www.mysunrise.ch/users/thhdesign/more.html

MyPod
www.clichesw.com/products/mypod/
Si connette a Internet e trasferisce su iPod news di siti a scelta, previsioni del tempo eccetera.

iSync
www.apple.com/isync
Sincronizza i calendari di iCal e i contatti di Rubrica Indirizzi su iPod.

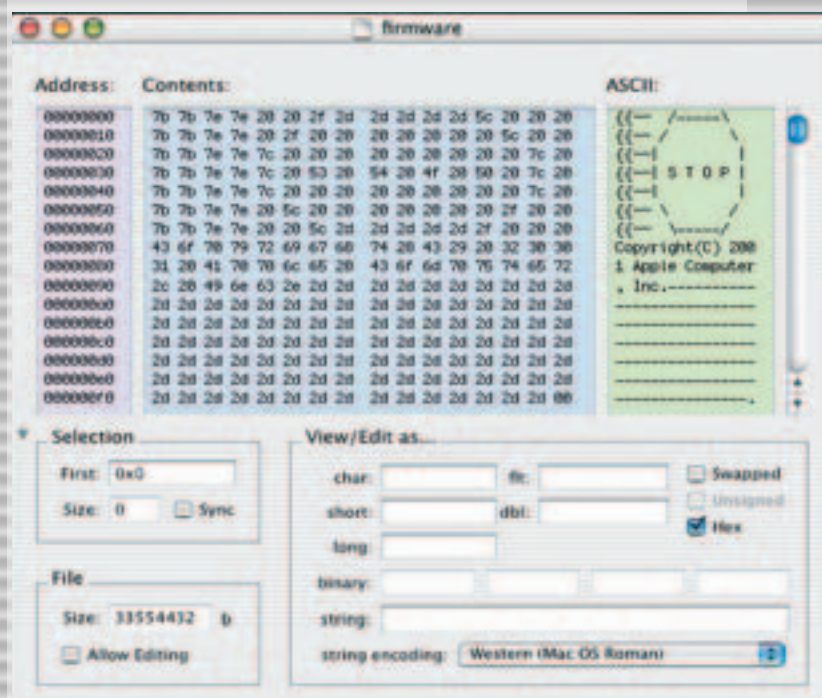
re meno scorrevole: la soluzione è **rimuoverla e pulirla per bene** (il problema non sussiste se si possiede la versione di iPod "no moving parts", in pratica con la rotella costituita da una specie di trackpad). Procuratevi un nastro adesivo abbastanza potente, un pezzo di carta qualsiasi e delle forbici. Ritagliate nella carta una "corona" abbastanza stretta da coprire i pulsanti esterni alla rotella. Tagliate quindi un pezzo di nastro adesivo lungo una decina di centimetri. Applicatelo sulla corona e fate aderire il tutto sui comandi. Dopo esservi accertati che il nastro adesivo abbia fatto ben presa, prendetelo ai bordi esterni e, tenendolo il più teso possibile, tirate verso l'esterno: con un "plop" la rotella si staccherà. Le quattro stanghette su cui questa appoggia, se non ben lubrificate, possono creare attrito. Cercate inoltre di eliminare l'eventuale polvere presente: vi consiglio un compressore o un phon (ad aria fredda). Prima di andare oltre, ricordatevi che **APRIRE iPOD INVALIDA LA GARANZIA.** Disponete dunque il lettore su un panno morbido e pulito e procuratevi un pezzo di plastica molto sottile: tenendo il lettore per la parte in acciaio (quella posteriore) spingete delicatamente la parte in plastica (quella anteriore) verso il basso e infilate il pezzo di plastica tra le due.

```
Terminal — tcsh (ttyp1)
[iMac:~] marco% mount
/dev/disk0s5 on / (local, journaled)
devfs on /dev (local)
fdesc on /dev (union)
<volfs> on /.vol (read-only)
automount -fstab [385] on /Network/Servers (automounted)
automount -static [385] on /automount (automounted)
/dev/disk1s3 on /Volumes/iPot (local, nodev, nosuid)
[iMac:~] marco% dd if=/dev/disk1s2 of=firmware
65536+0 records in
65536+0 records out
33554432 bytes transferred in 14.576172 secs (2302006 bytes/sec)
[iMac:~] marco% dd if=/dev/disk1s2 of=backup
65536+0 records in
65536+0 records out
33554432 bytes transferred in 15.267984 secs (2197699 bytes/sec)
[iMac:~] marco% dd of=/dev/disk1s2 if=firmware
65536+0 records in
65536+0 records out
33554432 bytes transferred in 41.109595 secs (816219 bytes/sec)
[iMac:~] marco% |
```

Gli interventi "a cuore aperto" sul firmware dell'iPod richiedono un po' di dimestichezza con l'uso dei comandi Unix da terminale.

Con questo dovete far scattare i piccoli "ganci" che tengono la cover anteriore legata alla posteriore: basta un po' di pazienza. Una volta aperto **ricordatevi di scollegare la batteria**.

>> Analisi del firmware

Il disco rigido di iPod è diviso in **3 partizioni**. La prima è di circa 32 KB e contiene informazioni relative a iPod. La seconda ha una capacità di 32 MB e ospita il firmware. La terza contiene musica, preferenze, calendari e contatti. Prima di iniziare, **backuppate tutti i file di iPod**. Collegate dunque il vostro lettore, aprite il Terminale e digitate **mount**, che ci restituirà la lista di tutti i volumi montati; in particolare dovreste poter leggere qualcosa di simile a **/dev/disk1s3 on /Volumes/iPot** che ci indica

che la terza partizione del disco interno di iPod (disco 1) è localizzata nella cartella Volumes; digitando **dd if=/dev/diskNs2 of=firmware** (dove **N** è il numero del disco di iPod, in questo caso 1), copieremo su computer la seconda partizione del disco 1 con il nome di "**firmware**". Vi consiglio di copiare il firmware una seconda volta con il nome di "**backup**" per poter, se necessario, ripristinare il lettore. Aprendo con un qualsiasi editor esadecimale (per esempio, **HexEditor**) il file **firmware**, potrete dare qualche "ritoccatina" al firmware. Salvate le modifiche, copiate il nuovo firmware su iPod con il comando **dd of=/dev/diskNs2 if=firmware**. Se, dopo tutto questo, iPod dovesse comportarsi in maniera anomala vuol dire che è arrivato il momento di ripristinare l'OS con l'utility di Apple "**iPod Software Updater**" oppure con il comando **dd of=/dev/diskNs2 if=backup**, cosa che eliminerà anche ogni prova della nostra colpevolezza.

Marco Triverio
trive@mac.com

23_25_hj28_at 11-06-2003 10:33 Pagina 23

Comandare il telefonino

Collegando il PC al cellulare, è possibile impartire comandi, inviare messaggi e modificare la rubrica. Ecco come fare...

Ormai quasi tutti i cellulari in circolazione sono costituiti da un modem interno, che può essere controllato con comandi AT, definiti come standard dall'ETSI (European Telecommunication Standard Institute - www.etsi.org) nei documenti GSM 07.07 e GSM 07.05.
I comandi AT+, oltre che per regolare le comunicazioni, **possono servire anche per accedere alle informazioni e funzionalità del proprio cellulare** come codice IMEI, rubrica, SMS eccetera.
Tramite i comandi AT possiamo:

- leggere i valori attualmente impostati, per esempio mandando il comando AT+CMGF=?;
- testare se un comando è supportato, sempre con AT+CMGF=?;
- impostare dei nuovi valori ai parametri dando ad esempio il comando AT+CMGF=0.

La linea di comando può essere costituita anche da diverse istruzioni separate da un ";".
Le possibili risposte dei comandi AT possono essere in formato numerico o testuale. Per impostare il formato possiamo usare:

- il comando ATV0 per il formato numerico;
- oppure ATV1 per il formato testuale.

>> Requisiti e impostazioni

Passiamo alla parte pratica: innanzitutto abbiamo bisogno di **un sistema per collegare il PC al telefono** (cavetto di collegamento, porta a infrarossi IRDA o Bluetooth) **e di un programma come Hyper Terminal di Windows oppure "minicom" di Linux**. Nell'esempio abbiamo utilizzato per la connessione un cavetto seriale fatto in casa, e faremo riferimento a minicom, ma le stesse operazioni possono essere eseguite con Hyperterminal.
Iniziamo subito con la **configurazione di minicom**. Per prima cosa apriamo un Terminale e digitiamo:

```
[korn@localhost korn]$ su
(invio)
Password:***** (invio)
[root@localhost korn]#mini
com -s (invio)
```

Figura 1

Il comando **su** serve per diventare root (non necessario su Windows), mentre **minicom -s** serve per configurare il programma. A questo punto apparirà una finestra come in **figura 1**.
La reale modifica da apportare è la configurazione della porta di comunicazione; selezioniamo con i cursori **Serial Port Setup** e premiamo **Invio** (**figura 2**), poi premiamo **A** e modifichiamo la porta di collegamento, che nel mio caso è **ttys1=com2**. Premiamo **Invio** due volte, salviamo la configurazione con **Save setup as...** (**figura 3**) e andiamo su **Exit**. Il programma chiuderà da solo la finestra di configurazione di minicom (**figura 4**), e se per caso avessimo selezionato **Exit from minicom**, basterà digitare nuovamente dal terminale **minicom**.
Ora non ci resta che testare se il collegamento funziona dando il comando **AT+CGMI** seguito da **Invio** (**figura 5**); come risposta otterremo il tipo di telefono in nostro possesso. Nel riquadro in queste pagine trovate un elenco dei comandi di uso più generale.

>> Controllare gli SMS

Passiamo ora ai comandi per la gestione degli SMS. Prima di iniziare cerchiamo di fare una piccola panoramica e di capire cosa sono esattamente i messaggi SMS... Come specificato dall'organizzazione di ETSI (i nuovi documenti

23_25_hj28_at 11-06-2003 10:33 Pagina 24

Figura 2

sono su www.etsi.org/download/) **il messaggio SMS può essere classificato a seconda dei bit dei caratteri**, infatti:

- **7-bit:** è un normalissimo messaggio lungo fino a 160 caratteri;
- **8-bit:** è lungo fino a 140 caratteri e non sono visti dai telefonini come messaggi di testo, ma vengono riconosciuti come immagini, loghi e toni di chiamata;
- **16-bit:** su alcuni telefonini compare come flash SMS.

Gli SMS possono essere letti in due modi:

- **PDU MODE** (protocol description unit): modalità a 7-bit in cui il testo viene espresso in forma esadecimale;
- **TEXT MODE**: il testo è espresso con caratteri alfabetici.

Qui analizzeremo un messaggio in ricezione nel formato "PDU MODE" poiché non tutti i cellulari supportano la funzione Text Mode. Comunque **per verificare se il nostro cellulare supporti il Text Mode**, possiamo dare il comando:

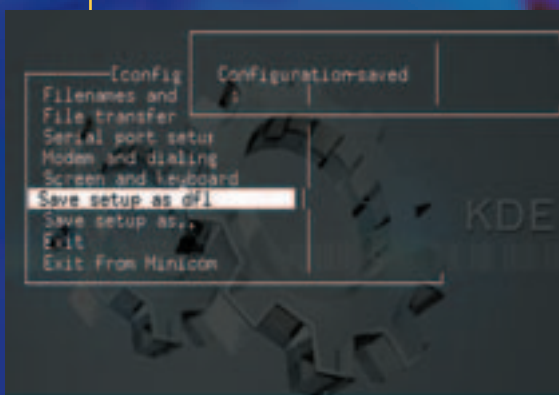



Figura 3

```
AT+CMGF=?
```

Se riceviamo come risposta:

```
+CMGF: (0)
```

allora la funzione TEXT MODE **non è supportata**; se invece di fianco allo "0" esce anche "1", allora possiamo tranquillamente leggere i messaggi in TEXT MODE dando il comando:

```
AT+CMGF=1
```

Supponendo che il nostro cellulare non supporti il TEXT MODE, dovremo cerca-

```
Welcome to minicom 2.00.0

OPTIONS: History Buffer, F-key Macros, Search History Buffer, I18n
Compiled on Jul 27 2002, 17:54:50.

Press CTRL-A Z for help on special keys

AT S7=45 S0=0 L1 V1 X4 &c1 E1 Q0
OK
```

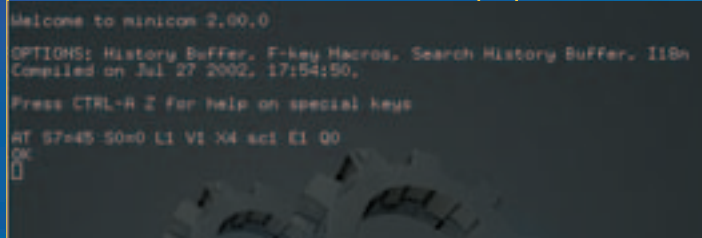



Figura 4

re di codificare la risposta che ci dà alla richiesta di lettura dei nostri messaggi. Per prima cosa, dobbiamo definire **su quale memoria leggere i messaggi**. Diamo il comando:

```
AT+CPMS=SM
```

Questo ci permetterà di impostare come memoria predefinita quella della **SIM**; nel caso volessimo impostare la memoria del cellulare come predefinita dovremmo sostituire "SM" con "ME". Una volta deciso a quale memoria fare riferimento, dobbiamo decidere quale tipo di messaggio vogliamo leggere. In effetti, ne esistono diversi tipi:

1. **"0"** messaggi ricevuti e non letti;
2. **"1"** messaggi ricevuti e letti;
3. **"2"** messaggi memorizzati e non inviati;
4. **"3"** messaggi memorizzati e inviati;
5. **"4"** tutti i tipi di messaggi.

Se decidiamo di optare per l'ultima opzione, e cioè leggere indistintamente tutti i messaggi, scriviamo questo comando:

```
AT+CMGL=4
```

La risposta a tale comando contiene tutti i tipi di messaggi presenti in questo momento nel nostro cellulare. Analizziamone qualcuno, per esempio:

```
at+cmgl=4
0791"932350585800"040C91"23
103254F6"    0000
30502050030340
04"C374F80D"
```

"07" riguarda la lunghezza del numero del centro servizi (SMSC) espressa in numero di ottetti;
"91" rappresenta il tipo del numero del centro servizi SMSC;
"93 23 50 58 58 00" sono i semi-ottetti decimali del numero del centro servizi, che in questo caso è quello della wind +39 320 5858500;
"04" è il primo ottetto del messaggio SMS-DELIVER;
"0C" è la lunghezza del numero del mittente;
"91" numero del centro servizi SMSC;
"23 10 32 54 F6" questo rappresenta il numero del mittente, e cioè 320 123456, la F viene aggiunta perché in questo caso la lunghezza del numero di telefono è dispari;
"00" TP-PID;

I COMANDI GENERALI

I vari comandi AT, come definiti dallo standard ETSI GSM 07.07.

AT+CGMI	Marca del telefono
AT+CGMM	Tipo di telefono
AT+CGMR	Versione GSM del telefono
AT+GSN	Codice IMEI
AT+CHUP	Termina la chiamata in corso
AT+CREG	Registrazione sulla rete
AT+CLCK	Modifica il blocco da ON ad OFF
AT+CPWD	Cambia la password del blocco
AT+CLIP	Mostra il numero chiamante
AT+CHLD	Gestisce più chiamate
AT+CBC	Stato di carica della batteria
AT+CSQ	Qualità del segnale di uscita
AT+CAOC	Avviso di ricaricare la batteria
AT+CIMI	Fornisce l'IMSI
AT+CLCC	Elenco delle chiamate correnti
AT+COPN	Legge i nomi degli operatori

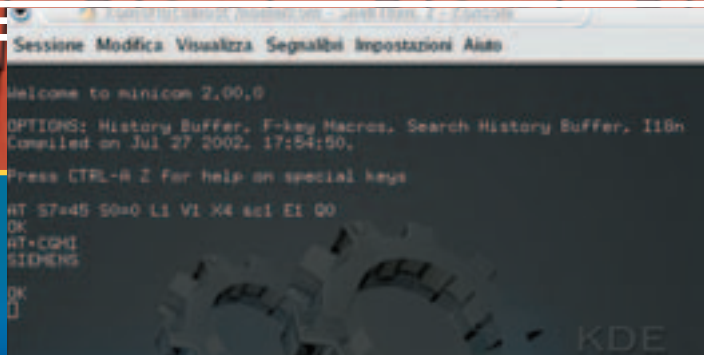



Figura 5

LA DATA DEGLI SMS

Considerando l'esempio riportato nel testo (30 50 20 50 03 03 40), la data e l'ora del messaggio hanno questo significato:

l'anno (30 —> 03 2000 + 03 = 2003);
il mese (50—>05 = maggio);
il giorno (20—>02);
l'ora (50—>05);
i minuti (03—>30);
i secondi (03—>30) di invio del messaggio;
l'ultimo 40 rappresentano il tempo-zona relativo al GMT;
Il TP-SCTS riportato rappresenta quindi la data ed ora 02/05/2003 05:30:30.

"00" TP-DCS;
"30 50 20 50 03 03 40" Questo è il campo TP-SCTS, che rappresenta il time stamp relativo all'invio del messaggio. Tutti i valori rappresentati sono composti da due cifre, e vengono rappresentati su un byte, composto dai due nibble

Figura 6

rappresentanti le due cifre invertiti nell'ordine. L'anno è rappresentato con l'offset rispetto all'anno 2000.
"04" TP-UDL rappresenta la lunghezza del messaggio;
"C3 74 F8 0D" questo rappresenta il corpo del messaggio "ciao", questo tipo di codifica consiste nel trasformare una sequenza di caratteri a 7 bit in una sequenza di byte. In riferimento alla figura 6, il carattere di sette bit è trasformato in un byte aggiungendo come bit più significativo il bit più a destra del secondo carattere, quindi una volta eliminato il bit più a destra del secondo carattere, per otterenere un nuovo byte, abbiamo bisogno dei due bit meno significativi del terzo carattere. Si continua a procedere in questo modo fino ad arrivare alla fine del messaggio.

>> Uso della rubrica

Passiamo ora alla gestione della rubrica. Per prima cosa dobbiamo decidere a quale rubrica riferirci. Anche in questo caso, infatti, ne esistono di tipo diverso:

1. SM è la rubrica standard della SIM;
2. ON è la rubrica dei numeri propri;
3. ME è la rubrica standard del telefono;
4. RC è la lista delle chiamate perse;
5. MC è la lista delle chiamate ricevute.

Quindi mandiamo il comando relativo alla rubrica che abbiamo scelto, ad esempio SM:

```
AT+CPBS=SM
```

dopodiché possiamo leggere (in questo caso) la rubrica relativa alla sim con il comando:

```
AT+CPBR=("inizio indice","fine indice")
```

Per esempio, con **AT+CPBR=1,100** verrà restituito un elenco di tutte le voci presenti nella rubrica dalla prima fino alla centesima voce, per modificare o cancellare si usa il comando:

```
AT+CPBW=10,4242,"wind"
```

dove 10 rappresenta la posizione in memoria, 4242 è il numero di telefono e wind la descrizione.

Nel caso si voglia cancellare la stessa voce basta mandare il comando:

```
AT+CPBW=10
```

senza mettere alcun numero o descrizione.

>> Sotto con la sperimentazione

Bene, se questa introduzione vi ha messo l'acquolina in bocca, non avete che da fare qualche esperimento. Tenete presente che alcuni cellulare potrebbero avere funzioni in più, o implementare in modo particolare alcuni dei comandi. In ogni caso, è sempre meglio fare **prima una copia dei numeri della rubrica** (non si sa mai...), e magari fare i primi esperimenti senza avere troppo credito sulla scheda (**per errore potreste chiamare in Australia...**).
Se volete saperne di più, potete fare riferimento al sito internet www.dreamfabric.com oppure www.mokabyte.it per quanto riguarda i messaggi in trasmissione e maggiori chiarimenti. Altre informazioni utili si trovano su www.siemens.com e www.nokia.it.

S.O.S. - KoRn
(dedicato a mio padre)

COMANDI PER LA GESTIONE DEGLI SMS

Comando	Descrizione
AT+CSMS	Selezione del messaggio di servizio
AT+CMGF	Formato degli SMS
AT+CSCA	Numero del centro servizio degli SMS
AT+CNMI	Mostra i nuovi SMS giunti
AT+CMGL	Lista degli SMS
AT+CMGR	Lettura di un SMS
AT+CMGS	Spedizione di un SMS
AT+CMGW	Scrittura di un SMS dalla memoria
AT+CMGD	Cancellazione di un SMS presente in memoria
AT+CMGC	Spedizione di un comando di un SMS

E LUCE FU!

Sul numero scorso abbiamo visto come progettare e tagliare una finestra nel case del PC; ora le daremo vita, con un'illuminazione particolare, e un'incisione.

Rivediamo un attimo quanto abbiamo detto fin qui: innanzi tutto abbiamo progettato una finestra con un programma di grafica, ne abbiamo ricavato una sagoma da applicare al PC per segnare i contorni della finestra, e abbiamo tagliato il case con uno strumento rotativo. La finestra è stata quindi chiusa con una lastra di plexiglas, tagliata anch'essa in misura, e fissata con una guaina in gomma.

Se vogliamo praticare sul plexiglas un'incisione a rilievo, che si illumini con la luce, lo spessore della lastra deve essere di 2 o 3 mm. Questo rende impossibile l'uso di una guaina ad H, in quanto la lamiera del case in genere è spessa non più di 1 mm. La guaina ad H inoltre in questo caso impedirebbe alla luce di illuminare l'incisione, in quanto essa "entra" proprio dai bordi della lastra di plexiglas.

Dal punto di vista pratico, realizzare un bassorilievo sul plexiglas, è abbastanza complicato. Si può avere un lavoro perfetto ricorrendo a strumenti di precisione, come il laser, ma se si ha molta pazienza e una buona manualità, si possono ottenere degli ottimi risultati anche fresando il materiale plastico con il Dremel.

>> In pratica...

Consapevoli di tutto questo, vediamo ora quali sono state le scelte per il nostro modding.

Per quanto riguarda la guarnizione, abbiamo modificato un tubicino in silicone semitrasparente, normalmente usato per portare miscela al carburatore nei modelli radiocomandati, iniettandoci della vernice verde metallizzata e incidendone un lato, una volta essiccato il colorante.

Volendo si può ottenere lo stesso effetto dei kit che sono in vendita presso molti siti web, usando la guarnizione del cofano motore delle Vespa, acquistabile presso qualsiasi negozio di ricambi per moto ben fornito, con una spesa ridicola (Grazie Nippo per la dritta!). Il risultato in questo caso è davvero molto buono.

Per fissare la finestra abbiamo usato delle viti con bulloni. Attenzione a scegliere le viti appropriate: non devono essere troppo lunghe, per non danneggiare le schede del PC, e con la testa preferibilmente conica, in modo da non creare uno spessore tra la lamiera ed il plexiglas, che può così andare a contatto con la guarnizione.

>> Illuminazione

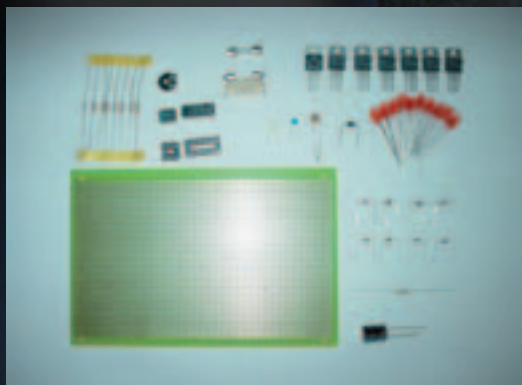
Le possibilità per portare un po' di luce sul lato oscuro del nostro case, sono davvero tante! Basta navigare un po' per rendersene conto. Neon a catodo freddo, neon normali adattati, stringhe luminose, lampadine di vario tipo, tubi fluorescenti, ventole con led incorporati e chissà cos'altro ancora... Ma quale scegliere? È sufficiente un giudizio estetico, o ci sono anche altri aspetti da tenere in considerazione?

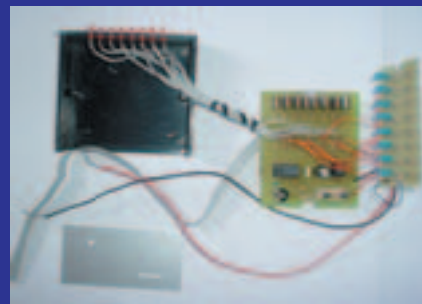
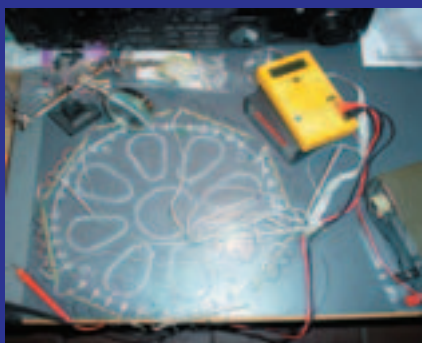
Noi, ad esempio, abbiamo preferito i

La fresatura del plexiglas con il Dremel può raggiungere risultati apprezzabili, ma è un lavoro molto meticoloso, che richiede tempo e molta pazienza.

Per assemblare il plexiglas al pannello, abbiamo incollato dei bulloni alla lamiera, con della colla al cianoacrilato a presa rapida, dopo aver "scarteggiato" le superficie a contatto.

In questo modo la finestra è facilmente smontabile per le modifiche e, allo stesso tempo, la zona esterna del pannello è rimasta sgombra.

led ad alta luminosità, perché costano poco (eccetto quelli blu -sigh!-), sono molto affidabili, consumano pochissima corrente, durano quasi in eterno, e si prestano molto bene ad essere controllati tramite semplici circuiti elettrici per ottenere effetti speciali di vario tipo. Con uno o due integrati, più una manciata di resistenze e condensatori, è infatti possibile realizzare il famigerato effetto Supercar, oppure uno strobo, un varilight, un lampeggiatore, ecc...

A questo punto però bisogna avere delle basi di elettronica, anche perché con un solo collegamento sbagliato, si corre il rischio di fulminare l'alimentatore del PC. In internet sono disponibili molti tutorial ed eBook al riguardo, e chi sa cercare bene, potrebbe riuscire anche a trovare gli schemi per questi semplici circuiti. Per il computer preso come modello in questo articolo, abbiamo realizzato due schede. La prima, semplicissima, è costituita essenzialmente da un timer 555, per comandare dei led rossi con un effetto strobo, da puntare sulla CPU. La seconda scheda, un po' più complicata, serve ad illuminare, con dei led gialli, i petali del fiore, in modo che si accendano uno dopo l'altro con una leggera scia.
Abbiamo poi dotato il PC di un neon a catodo freddo verde, con l'intento di vedere se conviene rispetto ad una soluzione "fatta in casa" con un neon tradizionale da 8 cm colorato a mano.
In questo caso, a nostro parere, non vale più la pena di lavorare tanto per realizzare un impianto di illuminazione a neon. Benché la luce del neon blu abbia un colore più intenso, quello verde risulta meno ingombrante e più gradevole esteticamente, non contribuisce al surriscaldamento del case, non crea interferenze elettromagnetiche (visto che lavora in corrente continua) e il costo è praticamente identico se non inferiore. Se non siete molto esperti con la corrente, consiglio di comprare un kit già pronto, che sarà dotato sicuramente anche dei connettori per spillare corrente direttamente dall'alimentatore del PC.

Le luci stroboscopiche, puntate sulla CPU.

Il controller per i led, che si illuminano in modo alternato.

I led colorati, montati sui petali della finestra.

Il neon a catodo freddo, di colore verde.

>> Alimentazione

L'alimentatore si rivela sempre più spesso un componente molto delicato, soggetto a continui sbalzi di tensione, e nella maggior parte dei casi al limite delle proprie potenzialità, a causa di processori molto esigenti, qualche HDD, masterizzatori, lettori DVD e periferiche.
Proprio per evitare di sovraccaricarlo o danneggiarlo, eventualità non così improbabile, visto il carattere sperimentale del nostro impiantino, abbiamo deciso di usare un alimentatore esterno, realizzando un pannellino di controllo sul retro del PC.
Questa soluzione permette di illuminare il case anche a computer spento, cosa che a volte può rivelarsi utile, ad esempio per sostituire HDD, impostare jumper o semplicemente fare un po' di pulizia.
Il modding a questo punto è concluso. Siamo riusciti a creare una finestra a forma di fiore, con una guarnizione semitrasparente con degli inserti verdi metallizzati, e un pannello di plexiglas con una fresatura che ricalca i petali del fiore, e questo è il risultato. Si poteva fare di meglio? Ne sono convinto, e mi aspetto che siate proprio voi a dimostrarlo! Il nostro intento era proprio di stuzzicare la vostra fantasia e di darvi, dove possibile, qualche dritta per concretizzare le vostre idee.

Spero che alla fine sia emerso come in realtà non sia così difficile customizzare radicalmente il proprio PERSONAL computer e che la qualità del risultato finale è subordinata alla soddisfazione personale di essere riusciti a fare quanto più possibile da soli, senza dover ricorrere necessariamente a dei kit commerciali.

G14N & M477

Verifica la sicurezza

Microsoft Baseline Security Analizer analizza i sistemi Windows a caccia di possibili problemi di sicurezza. Sistemarli tutti sarà come travasare il mare con un cucchiaino, ma almeno si possono eliminare i più importanti.

Nell'Ottobre del 2001, a soltanto un mese di distanza dalla tragedia delle due torri, i sistemi informatici basati su piattaforma Microsoft subivano l'attacco del virus Nimda. Quest'evento, unito alla precedente diffusione del virus Code Red, spinse Microsoft ad allestire il **Microsoft Strategic Technology Protection Program**. Oggetto tangibile di questo programma è l'utility **Microsoft Baseline Security Analyzer** che da questo momento in poi chiameremo **MBSA**.
In breve il MBSA **effettua vari controlli sempre relativi alla sicurezza su tutti i sistemi operativi Microsoft che implementino delle politiche di sicurezza**: Windows NT 4, Windows 2000, Windows XP (sono esclusi naturalmente i vari Windows 98/Me et similia). Lo scopo di quest'articolo è di vedere nel dettaglio il funzionamento del MBSA anche attraverso degli esempi.
Innanzi tutto scarichiamolo dal link fornito nell'apposito box in queste pagine. Dopodiché è opportuno verificare che il nostro computer o la nostra rete abbiano i requisiti adatti, ossia se oltre ad essere dotati dei sistemi operativi sopra citati, **abbiano installato anche Internet Explorer 5.01:** questo perché il MBSA ha bisogno di un parser XML. Chi non dovesse disporre di IE 5.01 può scaricarsi il MSXML versione 3.0 con SP2 dall'indirizzo nel box.

La pagina iniziale, da cui scegliere le varie opzioni.

Le opzioni di base

L'utilizzo del MBSA è molto semplice: nella prima schermata avete la possibilità di **effettuare lo scan di un singolo computer**, specificandone il nome o l'indirizzo IP, **oppure di un'intera rete**, specificandone il nome di dominio o il range di IP. Infine è possibile aprire report già elaborati. In entrambe le modalità di scansione si possono specificare i controlli da effettuare, che sono:

- Controllo delle vulnerabilità di Windows
- Controllo di password deboli
- Controllo delle vulnerabilità di IIS
- Controllo delle vulnerabilità di SQL
- Controllo dei security update

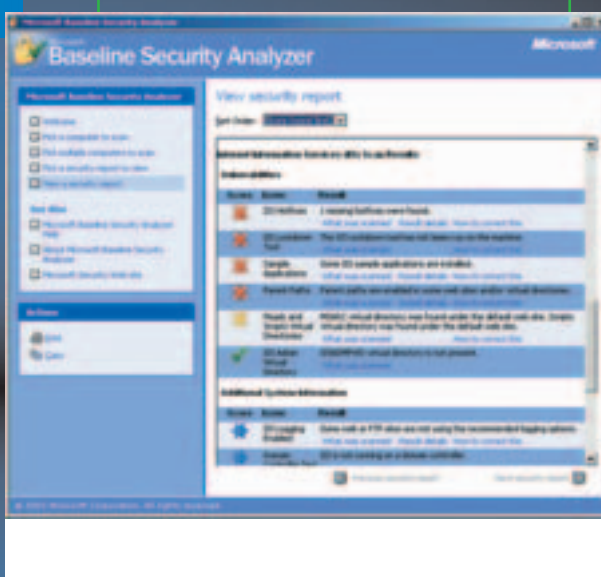
Quest'ultima opzione permette inoltre di specificare se si vuole fare riferimento all'elenco degli **aggiornamenti contenuti nel file mssecure.xml** che il MBSA scarica da Internet durante l'esecuzione, oppure se far riferimento ad un altro SUS (Software Update Service), per esempio relativo ad una sola realtà (azienda, ente etc.). Nell'ultima versione del MBSA vengono inoltre controllati i security update di eventuali versioni di **Exchange** e **Windows Media Player** installati.
Il MBSA può essere utilizzato **anche da linea di comando** attraverso l'eseguibile **mbsacli.exe**, che da maggiori

Gli avvisi con le patch più critiche, correzioni da apportare con una certa urgenza.

opzioni all'utente, come spesso accade nelle versioni console degli applicativi. La schermata dell'help del programma potete richiamarla con questa linea di comando:

```
mbsacli.exe /? >
mbsahelp.txt
```

28_31_hj28_mbsa 11-06-2003 10:40 Pagina 29

di Windows

Con l'espressione > mbsahelp.txt si può indirizzare l'output su un file di testo, in modo che sia più facile da leggere.

Come potete notare nel riquadro alla fine, vengono indicate le impostazioni di default con cui parte la versione GUI di MBSA cioè l'opzione **s 2**, che sopprime le note e i warning degli update di sicurezza, e le opzioni nosum e baseline, che servono rispettivamente ad evitare il controllo sul checksum dei file da aggiornare ed a **fare in modo che si controllino esclusivamente le patch di sicurezza catalogate come critiche**. Da linea di comando è inoltre possibile diversificare lo stile di scansione; per esempio, con l'opzione **hf** che consente di utilizzare lo stile del vecchio HFNetChk, un'utility che effettuava esclusivamente il controllo sugli aggiornamenti.

I controlli sul sistema

Vediamo adesso in dettaglio la descrizione dei controlli del MBSA:

Controllo delle vulnerabilità di Windows consiste in vari controlli tra cui:

- la ricerca dell'**appartenenza degli utenti al gruppo Administrators**. Se vi sono più di due utenti appartenenti a questo gruppo viene segnalata una possibile vulnerabilità.
- Il controllo dell'auditing cioè **se è impostata la registrazione di eventi** quali i logon degli utenti avvenuti con successo e i tentativi di accesso falliti.
- Il **controllo dell'autologon** verifica l'avvenuta attivazione di quest'opzione che consente l'accesso ad un sistema senza autenticazione e segnala una grave vulnerabilità quando la password di logon, che si trova nel registro di configurazione, è conservata come testo in chiaro. Nel caso di password cifrata la vulnerabilità viene considerata potenziale.
- Il **controllo dei servizi non necessari** verifica se i servizi contenuti nel file services.txt sono abilitati. L'utilità di quest'operazione è la possibilità di stabilire su un'intera rete un unico elenco di servizi da considerarsi non necessari.
- Il **controllo dell'utente Guest**. Nei sistemi Windows 2000 e NT l'abilitazione di quest'utente viene considerata una vulnerabilità. Nei sistemi XP che usano il simple file sharing invece no, perché in questo caso la presenza dell'utente Guest è necessaria, anche se l'utilizzo stesso del simple file sharing andrebbe considerata come vulnerabilità.
- Il **controllo delle password locali** verifica se vi siano utenti con pas-

Eventuali problemi di Internet Information Services.

CONTROLLO SUGLI APPLICATIVI DESKTOP

I controlli dell'MBSA relativi agli applicativi desktop riguardano Internet Explorer, Office e Outlook.. Come probabilmente saprete, in IE esistono 4 zone di contenuti web: Internet, intranet locale, siti con restrizioni, siti attendibili. Per ognuna di queste è possibile impostare dei criteri di sicurezza. Il MBSA, oltre a rilevare le impostazioni correnti, e se esse sono eventualmente poco sicure, da dei consigli su come ottimizzarle. Stesso controllo viene effettuato in Outlook. Per quanto riguarda Office invece vengono registrate le configurazioni relative ai livelli di protezione sulle macro.

OPZIONI DA LINEA DI COMANDO

Queste funzionalità dell'MBSA possono essere attivate aggiungendo le opzioni corrispondenti al comando mbsacli.exe

OPZIONE	FUNZIONALITÀ
/c domain\computer	Analizza il computer specificato.
/i IP	Analizza l'indirizzo IP specificato.
/r IP-IP	Analizza il range di indirizzi IP specificati.
/d domain	Analizza il dominio indicato.
/n option	Seleziona le scansioni da NON eseguire. Tutti i controlli vengono eseguiti di default. Valori validi: "OS", "SQL", "IIS", "Updates", "Password". Possono essere concatenati con "+" (senza spazi).
/o filename	Modello XML per il file dei risultati. Default: %domain% - %computername% (%date%).
/f filename	Ridirige l'uscite su un file di testo.
/qp	Non visualizzare la progressione della scansione.
/qe	Non visualizzare la lista degli errori.
/qr	Non visualizzare la lista del rapporto.
/s 0	Non sopprimere le note e avvisi sugli aggiornamenti di sicurezza.
/s 1	Sopprimi le note sugli aggiornamenti di sicurezza.
/s 2	Sopprimi le note e gli avvisi sugli aggiornamenti di sicurezza.
/baseline	Esamina solo gli aggiornamenti di sicurezza di base.
/nosum	I controlli sugli aggiornamenti di sicurezza non esamineranno i checkum dei file.
/sus	SUSserver Verifica solo gli aggiornamenti di sicurezza approvati sul server SUS specificato. SUS implica /nosum; includere /sum dopo l'opzione /sus per scavalcare l'impostazione di default.
/e	Elenca gli errori dall'ultima scansione.
/l	Elenca tutti i rapporti disponibili.
/ls	Elenca i rapporti dall'ultima scansione.
/lr filename	Visualizza un rapporto riassunto.
/ld filename	Visualizza un rapporto dettagliato.
/v	Visualizza i codici degli aggiornamenti di sicurezza.
/hf Hotfix Checker	Esegui in modalità HFNetChk. Lanciare con /hf -? per l'help di hfnetchk. Il parametro /hf deve essere il primo parametro nella linea di comando.
/?	Visualizza l'help (in inglese).

sword vuote oppure che siano uguali al nome utente o che siano password semplici del tipo: 'password' o 'admin' o ancora 'administrator'. Segnala inoltre se vi sono account disabilitati o bloccati (come avviene nel caso in cui vi siano stati troppi tentativi di logon senza successo). Il MBSA effettua questa verifica cercando di modificare tutte le password. Naturalmente il cambiamento non è permanente ma porta esclusivamente alla notifica della presenza di password troppo semplici.

I risultati di una scansione su un PC possono essere visualizzati in vari modi, per evidenziare eventuali problemi.

• Il **controllo della scadenza delle password**. Una password che non è sottoposta a scadenza viene considerata una vulnerabilità.
• Il **controllo della chiave di registro RestrictAnonymous** utilizzata per limitare le connessioni anonime è fonte di numerose informazioni per i malintenzionati, come abbiamo visto in un precedente articolo di HJ.

Infine vengono comunicata alcune informazioni quali la **versione del sistema operativo**, il **tipo di file system utilizzato** (NTFS o FAT), le **cartelle condivise**.

Sicurezza del Web

Il MBSA non si limita però al controllo sulle vulnerabilità del sistema operativo, ma come abbiamo detto **è in grado di controllare anche IIS**. I controlli su IIS sono i seguenti:

• Il controllo della **presenza di MSADC e delle Scripts Virtual Directories**. Queste directory in genere contengono degli script di accesso ai dati che è opportuno eliminare se non vengono utilizzate. Un'utility che si occupa della chiusura delle funzionalità non utilizzate è la IIS Lockdown compresa nel Microsoft Security Tool Kit.
• Il controllo della **presenza della cartella virtuale IISADMPWD**. Questa cartella viene utilizzata dagli utenti per la modifica delle password in via di scadenza.
• Verifica della **presenza di IIS su un controller di Dominio**. Questa pratica è in generale sconsigliata e per questo il MBSA la rileva come vulnerabilità: di norma il Domain Controller di una rete contiene l'elenco di tutti gli account degli utenti ed è quindi preferibile che non sia accessibile dall'esterno o che quantomeno non sia esposto all'accesso pubblico come un server web. Inoltre la sola presenza di

Da qui si possono scegliere i computer della rete da analizzare, per nome, dominio, numero IP o range di indirizzi.

Per ogni problema, può essere visualizzata una descrizione piuttosto approfondita.

LINK UTILI

www.microsoft.com/security/mstpp.asp
Sito del Microsoft Strategic Technology Protection Program

www.microsoft.com/TechNet/Security/tools/tools/MBSAHome.asp
Sito dell'MBSA. Qui troverete anche i link per scaricare il MBSA stesso o il MSXML 3.0 se avete una versione di IE precedente alla 5.01

www.microsoft.com/TechNet/Secutity/tools/tools/mbsaqa.asp
Sito delle FAQ su MBSA

http://www.securityfocus.com/infocus/1649
Articolo di Mike Fahland ed Eric Shultze sull'MBSA pubblicato su Security Focus

IIS, indipendente dal fatto che in esso risieda il sito pubblico dell'azienda, espone il server ad un rilevante quantitativo di vulnerabilità tipiche del server web di Microsoft.

- Il controllo dell'**abilitazione del logging su IIS**. Il logging è necessario per la registrazione di tutte le attività svolte dagli utenti sul server web e quindi per risalire all'origine di alcuni comportamenti "anomali".
- Il controllo delle **applicazioni d'esempio su IIS**. Questo controllo verifica la presenza delle seguenti cartelle sul sistema scandito:

```
o\Inetpub\iissamples
o\winnt\help\iishelp
o\Program Files\common files\system\msadc
```

Controlli su SQL

I controlli effettuati su SQL server sono quasi speculari ai controlli sulle vulnerabilità di Windows. Anche in questo caso vengono infatti rilevati gli **utenti appartenenti al ruolo di amministratore**, vengono controllate le **password degli utenti SQL** affinché non siano vuote, uguali al nome utente o troppo semplici; viene verificato se il **diritto di CmdExec è limitato al Sysadmin**, se l'utente **Guest** ha accesso ai database, se SQL server **si trova su un Domain controller**. Dopodiché vengono effettuati anche dei controlli specifici per SQL come ad esempio il tipo di autenticazione utilizzato. In un Server SQL, infatti, è possibile autenticare gli utenti in due modi: o **con l'autenticazione di Windows**, ossia all'utente autenticato sul sistema operativo viene dato anche accesso ai database (in questo caso si parla di trusted connection), oppure con il **metodo misto,** che viene utilizzato qualora il client non sia in grado di gestire connessioni NTLM o Kerberos. In questo caso è SQL Server a richiedere nome utente e password e a registrarli nelle sue tabelle di sistema.

Il MBSA rileva inoltre se il gruppo **BUILTIN\Administrators** (gruppo creato al momento dell'installazione di SQL Server) ha mantenuto le impostazioni di default ossia ha mantenuto il Sysadmin Role che da diritto di accesso su tutti i database del sistema. Vengono inoltre controllate le seguenti cartelle:

```
· Program Files\Microsoft SQL Server\MSSQL$InstanceName\Binn
· Program Files\Microsoft SQL Server\MSSQL$InstanceName\Data
· Program Files\Microsoft SQL Server\MSSQL\Binn
· Program Files\Microsoft SQL Server\MSSQL\Data
```

In particolare vengono verificate le loro **Access Control List** affinché non sia consentito l'accesso ad utenti che non siano l'Amministratore o gli account dei servizi SQL. Vengono infine controllate le chiavi di registro di SQL server relative alla sicurezza:

```
HKLM\Software\Microsoft\Microsoft SQL Server
HKLM\Software\Microsoft\MSSQLServer
```

Se il gruppo **Everyone** possiede più della possibilità di lettura su queste chiavi viene segnalata una vulnerabilità di livello alto. Oltre a controllare gli applicativi tipici di un server il MBSA controlla alcune applicazioni Desktop come potete leggere più approfonditamente nell'apposito riquadro.

Roberto 'decOder' Enea